

3 UNITED STATES OF AMERICA, - Docket No. 3:06-CR-719
4 Plaintiff, - Toledo, Ohio
5 v. - May 15, 2008
6 MOHAMMAD ZAKI AMAWI, et al. , - Trial
7 Defendants. -

8 VOLUME 51, TRANSCRIPT OF TRIAL
9 BEFORE THE HONORABLE JAMES G. CARR
UNITED STATES DISTRICT CHIEF JUDGE, AND A JURY

APPEARANCES:

12 For the Plaintiffs: United States Attorneys' Office
13 By: Thomas E. Getz
14 Justin E. Herdman
801 Superior Avenue, W
Cleveland, OH 44113
(216) 622-3840

15 U.S. Department of Justice
16 By: Jerome J. Teresinski
17 David I. Miller
10th & Constitution Ave, NW
Washington, DC 20530
(202) 353-3464

25

乙

25

1 For the Defendant Amawi: Office of the Federal Public

Defender - Cleveland

2 By: Amy B. Cleary

3 Jonathan P. Witmer-Rich

4 Edward G. Bryan

5 Timothy C. Ivey

6 750 Skylight Office Tower

7 1660 West Second St.

8 Cleveland, OH 44113

9 (216) 522-4856

10 Muawad & Muawad

11 By: Elias Muawad

12 36700 Woodward Avenue, Suite 209

13 Bloomfield Hills, MI 48304

14 (248) 594-4700

15 For the Defendant Kerger & Kerger

16 El-Hindi: By: Stephen D. Hartman

17 Suite 201

18 33 South Michigan Street

19 Toledo, OH 43602

20 (419) 255-5990

21 Boss & Vitou

22 By: Charles M. Boss

23 111 West Dudley Street

24 Maumee, OH 43537-2140

25 (419) 893-5555

26 Raslan, El-Kamhawy & Pla

27 By: Alek H. El-Kamhawy

28 Suite 3FE, 1700 East 13 Street

29 Cleveland, OH 44114

30 (216) 928-1500

31 For the Defendant David L. Doughten

32 Mazloum: 4403 St. Clair Avenue

33 Cleveland, OH 44103-1125

34 (216) 361-1112

35 Helmick & Hoolahan

36 By: Jeffrey J. Helmick

37 2nd Floor

38 1119 Adams Street

39 Toledo, OH 43624-1508

40 (419) 243-3800

41 25

1

Mohammed Abdrabboh
1620 Ford Avenue
Wyandotte, MI 48192
(734) 283-8405

2

3 Court Reporter: Tracy L. Spore, RMR, CRR
4 1716 Spielbusch Avenue
5 Toledo, Ohio 43624
(419) 243-3607

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24 Proceedings recorded by mechanical stenography, transcript
25 produced by notereading.

1 (Reconvened at 8:41 a.m.)

2 THE COURT: On your chair is something called jury
08:41:25 **3** instructions. I had hoped to be able to give these to you
08:41:28 **4** earlier in the case. You can keep these. During the course
08:41:37 **5** of the trial as various terms are mentioned you're entirely free
08:41:44 **6** to look at them and refresh your recollection as to what various
08:41:44 **7** terms mean. What these are, in a moment -- please don't read
08:41:51 **8** ahead -- in a moment I will read them to you. You can follow
08:41:55 **9** along, you can mark them up however you wish. I'll try to
08:41:55 **10** pronounce various terms and names correctly, but I'll do the
08:41:55 **11** best I can.

12 What these are are definitions of various terms.

08:42:07 **13** Some are people, some are Arabic words, some are locations.
08:42:07 **14** And the parties, I want to commend them because they worked
08:42:07 **15** quite diligently to reach an agreement as to these terms. And
08:42:23 **16** these are simply definitions that the parties have agreed I can
08:42:29 **17** read to you. And I will do so now.

08:42:32 **18** Ladies and gentlemen of the jury, you have heard

08:42:35 **19** certain terms during the presentation of the evidence that may
08:42:35 **20** be unfamiliar to you. To assist you in performing your job as
08:42:35 **21** the fact-finders in this case, the following stipulations have
08:42:35 **22** been agreed to by the prosecutors and counsel for the
08:42:51 **23** defendants. You can consider this information as evidence.

08:42:56 **24** The definitions of these terms, names, and events are relevant
08:42:56 **25** and unique to the facts of this case only. You will notice

1 that a few of these terms define religious or political
08:43:11 2 movements, for which there are obviously more expansive
08:43:15 3 explanations. All parties agree, however, that it is important
08:43:19 4 to at least give you some basic information concerning these
5 terms.

6 Additionally, these definitions do not represent
7 the official policy positions of the U.S. Government, nor do any
8 of these stipulations apply to future criminal or civil
9 litigation to which the government may be a party.

10 We expect that providing you with this information
11 will help you in making a decision in considering the evidence
08:43:46 12 as it relates to the law in this particular case. As with any
13 other evidence, either side may make use of these definitions
08:43:56 14 during their closing arguments. Again, it is entirely within
15 your province to consider this evidence within the context of
08:44:05 16 all the evidence in the case.

17 Stipulations - terms, names, and events listed by
18 topical area.

19 Geographical locations.

20 1. Abu-Ghraib: A city in Iraq located just west
21 of Baghdad in which is located a prison that was used by the
08:44:31 22 regime of Saddam Hussein and thereafter by Coalition Forces as a
23 detention facility.

24 2. Al Karmah: A town located in Iraq's Anbar
25 Province near Fallujah.

- 1 3. Anbar Province: Largest province in Iraq that
- 2 comprises most of the Western part of Iraq. The region is
- 3 predominantly Sunni.

00:00:15 **4** 4. Chechnya: Republic in southwestern Russia.

-08:-44:-46 5 In the mid 1990s, Chechnya became a key battleground for Islamic
00:00:26 6 militants and this area engaged in armed rebellion against the
-08:-44:-46 7 Russian government. In 1997, Islam became the state's official
00:00:36 8 religion.

00:00:37 9 Fallujah: A city in Iraq located approximately 40

-08-44-46 **10** miles west of Baghdad. Fallujah was the site of two battles

-08-44-46 11 between Iraqi insurgents and the U.S. military in April 2004 and

00:00:53 **12** November of 2004. The November 2004 battle resulted in the

-08-44-46 13 recapture of Fallujah from insurgency, from insurgent fighters.

00:01:10 **14** Haifa Street in Baghdad: A two-mile stretch of
00:01:14 **15** road in central Baghdad that has been a hotbed of insurgent

00:01:19 **16** activity against the military convoys of Coalition Forces.

00:01:24 17 Indonesia: A country located off the southeast

¹⁸ coast of the Asian mainland. Indonesia, a non-Arab country, is the world's fourth most populous nation.

19 possesses one of the largest Muslim populations of any country.

30 in the world. Between 85 to 90 percent of the population is

21. Management of which one Group?

32

22. **Modernization, Technological Change, and Capitalist Industrialization**

24 Kuwait, Iran, Turkey, Syria, Jordan, and Saudi Arabia. Iraq's

00:01:58 **25** the two largest ethnic groups are Arabs and Kurds. Other distinct

00:02:13 **1** Arabic is the most commonly spoken language. Kurdish is spoken
00:02:17 **2** in the north, and English is the most commonly spoken Western
00:02:21 **3** language. The majority, (60 to 65 percent) of Iraqi Muslims
-08:-44:-46 **4** are members of the Shi'a (Shiite) sect, but there is a large
00:02:33 **5** Sunni population as well made up of both Arabs and Kurds.
-08:-44:-46 **6** Small communities of Christians, Jews, Bahais, Mandaeans and
00:02:43 **7** Yeziis also exist. Most Kurds are Sunni Muslim but differ from
-08:-44:-46 **8** their Arab neighbors in language, dress, and customs.
-08:-44:-46 **9** Today, three somewhat distinct geographical regions
00:02:59 **10** exist in Iraq: One region in the north, (principal cities:
-08:-44:-46 **11** Irbill, Mosul and Kirkuk. Irbill is predominantly populated by
-08:-44:-46 **12** ethnic Kurds; Mosul consists of a mix of Sunni, Kurdish, some
00:03:16 **13** Shi'a, and other groups; while Kirkuk has mix of Kurds and other
-08:-44:-46 **14** groups); a second region in central and western Iraq that
00:03:26 **15** predominantly consists of Sunnis, (principal cities: Baghdad
-08:-44:-46 **16** and Fallujah); and a third region in the south, (principal city:
-08:-44:-46 **17** Basra), that is predominantly populated by Shi'a.
00:03:40 **18** Karbala: A city in Iraq approximately 55 miles
00:03:44 **19** southwest of Baghdad. Karbala is a city of historical and
-08:-44:-46 **20** religious significance to Shiites.
-08:-44:-46 **21** Karkuk: Alternatively pronounced Kirkuk, it is a
00:03:56 **22** city in Iraq located approximately 145 miles north of Baghdad.
00:04:01 **23** Kashmir: Region in the northwestern Indian
-08:-44:-46 **24** subcontinent bordered by China, Afghanistan, and Pakistan.
00:04:12 **25** Possession of the region is disputed between Pakistan and India.

-08:-44:-46 **1** Khalidiyah --

00:04:18 **2** Is that a correct pronunciation?

00:04:22 **3** MR. TERESINSKI: Khalidiyah.

00:04:24 **4** THE COURT: -- a city located in Iraq's Anbar

00:04:27 **5** Province near Ramadi.

00:04:31 **6** Mosul: A city in Iraq approximately 225 miles

00:04:36 **7** northwest of Baghdad.

00:04:38 **8** Palestine (Arabic: Filistin): Used by some in

00:04:42 **9** this case, in the context of the Israeli-Palestinian conflict,

00:04:47 **10** as a description of a geographical area in the Middle East, the

-08:-44:-46 **11** boundaries of which are the subject of deep political dispute.

-08:-44:-46 **12** Many Muslims believe this land to be occupied. This

00:04:58 **13** geographical area includes the Gaza Strip (including the city of

-08:-44:-46 **14** Rafah), and the West Bank (an area that lies to the west of the

-08:-44:-46 **15** country of Jordan, across the Jordan River.)

00:05:13 **16** What's the correct pronunciation?

-08:-44:-46 **17** MR. TERESINSKI: Radwaniyah.

00:05:19 **18** THE COURT: The site of one of Saddam Hussein's

00:05:24 **19** former presidential palaces and his main residence. Radwaniyah

-08:-44:-46 **20** is located adjacent to the Baghdad International Airport.

00:05:34 **21** Ramadi: A city in Iraq approximately 70 miles west

-08:-44:-46 **22** of Baghdad. Ramadi is the capital of the Anbar Province.

00:05:47 **23** Taji. A town in Iraq located approximately 20

-08:-44:-46 **24** miles north of Baghdad. A large military base and airfield is

-08:-44:-46 **25** located there.

00:05:56 **1** Tal Afar: A city in northwestern Iraq

00:06:00 **2** approximately 30 miles west of Mosul.

00:06:04 **3** Tikrit: A city in Iraq located approximately 100

00:06:08 **4** miles northwest of Baghdad. Tikrit is the birthplace of Saddam

00:06:13 **5** Hussein.

00:06:14 **6** Yusufiya: A township in Iraq's Babil province

-08:-44:-46 **7** approximately ten miles southwest of Baghdad.

00:06:23 **8** The second general topical set of instructions is

-08:-44:-46 **9** of Arabic and Islamic terms.

00:06:33 **10** Al Sham: The traditional Arabic term "Bilad

-08:-44:-46 **11** al-Sham" is a name for the region that today contains Syria,

-08:-44:-46 **12** Jordan, Lebanon, Israel, and the area publicly reported to be

-08:-44:-46 **13** controlled by the Palestinian Authority.

-08:-44:-46 **14** Ashary: A school of early Muslim speculative

-08:-44:-46 **15** theology founded by the theologian Abu Al-Hasan al-Ashari. It

00:07:04 **16** is reported that the Asharite view considered the comprehension

00:07:10 **17** of the unique nature and characteristics of God as being beyond

00:07:14 **18** human capability, and that while man had free will, he had no

00:07:19 **19** power to create anything.

00:07:20 **20** Caliph: Title of a Sunni Islamic leader, literally

00:07:27 **21** "successor", used to denote a political and military leader in

00:07:32 **22** the Sunni Muslim world.

00:07:34 **23** Dawa: An Arabic word meaning call or invite,

00:07:38 **24** including inviting people to Islam.

00:07:41 **25** Deen: Arabic word meaning religion or belief.

00:07:45 **1** Fatwa: Rulings of Islamic law.

-08:-44:-46 **2** Fitnah: An Arabic word with various meanings, including temptation, trial, or fascination. The term has been used to collectively refer to temptations or persecutions that

00:07:54 **3** Muslims may endure through their faith. The term has also been

-08:-44:-46 **4** used to refer to the period of division in Islam; for example,

00:08:07 **5** the internal struggle that resulted in civil war and religious

00:08:12 **6** schism between the Sunnis and Shi'a (circa AD 656 to 661).

00:08:29 **7** Hadith: A collection of sayings and deeds

00:08:36 **8** attributed to the Prophet Mohammed, which, along with the

00:08:40 **9** Qur'an, form the basis of the Islamic faith.

00:08:43 **10** Hajj: Obligatory Muslim pilgrimage to Mecca.

-08:-44:-46 **11** Halal: Arabic legal term that identifies those

-08:-44:-46 **12** acts and deeds that are permitted.

00:09:02 **13** Haram: Arabic legal term that identifies those acts

00:09:07 **14** and deeds that are forbidden.

-08:-44:-46 **15** Hijab: This word primarily refers to an article of

-08:-44:-46 **16** clothing used to cover a woman's head and body.

-08:-44:-46 **17** Islam: One of the world's major religions.

00:09:22 **18** Jihad: From the Arabic root means "to strive, to

-08:-44:-46 **19** exert, to fight." Jihad's exact meaning depends on the context

00:09:32 **20** in which it is used. It may express a struggle against one's

00:09:36 **21** evil inclinations, an exertion to convert non-believers, or a

00:09:42 **22** struggle for the moral betterment of the Islamic community. If

-08:-44:-46 **23** used in a religion context, the adjective "Islamic" or "holy" is

00:09:54 1 added. Jihad is the only legal warfare in Islam and it is
-08:-44:-46 2 carefully controlled in Islamic law. It must be called by a
00:10:03 3 duly constituted state authority, and preceded by a call to
-08:-44:-46 4 Islam or treaty, and non-combatants must not be attacked.
00:10:13 5 Extremists have branded some as "un-believers" for their alleged
-08:-44:-46 6 neglect in adhering to and enforcing a particular interpretation
-08:-44:-46 7 of Islam, and have justified conducting jihad to justify the
00:10:28 8 struggle against their co-religionists.

- 08:-44:-46 **9** Today, contemporary thinking about jihad offers a
- 08:-44:-46 **10** wide spectrum of views, including conservatives who look to
- 08:-44:-46 **11** classical Islamic law on the subject and radicals who promote a,
- 00:10:46 **12** quote, "violent jihad," close quote, against Muslims and
- 08:-44:-46 **13** non-Muslims.

00:10:52 **14** Mujahadeen: Plural form of the Arabic word

00:10:58 **15** mujahid, or, quote, "one who engages in jihad," close quote.

00:11:03 **16** Muslims: Believers or adherents to the Islamic

-08:-44:-46 **17** faith.

00:11:08 **18** Qur'an: The book of Islamic revelation. The

00:11:17 **19** Qur'an is believed by those of the Islamic faith to be the word

-08:-44:-46 **20** of God transmitted through the Prophet Mohammed.

00:11:29 **21** Ramadan: A Muslim religious observance that takes
00:11:34 **22** place during the ninth month of the Islamic calendar, believed
-08:-44:-46 **23** to be the month in which the Qur'an began to be revealed.

00:11:42 **24** Salafism: The principal tenet of Salafism is that
-08:44:46 **25** Islam was perfect and complete during the days of Muhammad and

-08:-44:-46 1 his companions, but that undesirable innovations have been added
-08:-44:-46 2 over the later centuries due to materialistic and cultural
00:12:05 3 influences. Salafism seeks to revive a practice of Islam that
-08:-44:-46 4 more closely resembles the religion during the time of Muhammad.

-08:-44:-46 5 Salafism has also been described as a simplified version of
00:12:21 6 Islam, in which adherents follow a few commandments and
-08:-44:-46 7 practice. Adherents to Salafism are referred to as Salafis.

-08:-44:-46 8 Shaheed: Martyr. Mujahidin who have earned a
-08:-44:-46 9 place in paradise through death in jihad.

-08:-44:-46 10 Sheikh or sheik: An Arabic title of respect akin
-08:-44:-46 11 to "sir".

00:12:42 12 Shi'a. Shiites. A minority denomination of
00:12:49 13 Islam.

-08:-44:-46 14 Sufi: Generally described as the "inner or
00:12:54 15 mystical dimension" of Islam. Sufis believe that it is
00:12:58 16 possible to become close to God and to experience this
00:13:01 17 closeness - while one is alive. The chief aim of all Sufis
-08:-44:-46 18 then is to let go of all notions of duality, including a
-08:-44:-46 19 conception of an individual self, and to realize the Divine
-08:-44:-46 20 unity.

00:13:15 21 Sunni: A majority denomination of Islam.

00:13:19 22 Ummah: The collective Muslim community throughout
-08:-44:-46 23 the world.

00:13:29 24 The next set of definitions is of groups,
00:13:35 25 organizations and institutions.

00:13:37 **1** Al Azhar University: A prominent Islamic
00:13:41 **2** university located in Cairo, Egypt.
-08:-44:-46 **3** Al Bara's Ibn Malek Brigade. Unit of Abu Musab Al
00:13:52 **4** Zarqawi's network dedicated to committing suicide missions in
-08:-44:-46 **5** Iraq.
00:13:57 **6** Al Mujahidin Army: Sunni insurgent group
00:14:02 **7** committing terrorist attacks in Iraq.
00:14:05 **8** Al-Neda Center for Islamic Studies and Research: Al
00:14:10 **9** Qaeda's former official website.
00:14:14 **10** Al-Qaeda: An Arabic word meaning "the base". Al
-08:-44:-46 **11** Qaeda is a U.S.-designated terrorist organization lead by Usama
00:14:28 **12** Bin Laden. That is sometimes spelled with an O, "Osama Bin
00:14:34 **13** Laden".
00:14:35 **14** Al-Qaeda in Iraq: A U.S.-designated terrorist
00:14:40 **15** organization previously lead by Abu Musab Al Zarqawi that
00:14:45 **16** conducts sniper, mortar, rocket, and improvised explosive device
00:14:50 **17** (IED) attacks on Coalition Forces in Iraq. The group was
00:14:54 **18** formerly known as Tawhid wal-Jihad, and has also claimed the
00:14:59 **19** responsibility for beheadings.
00:15:02 **20** Al-Qaeda in the Arabian Peninsula: An Al Qaeda
00:15:08 **21** affiliated group based in Saudi Arabia that has carried out
00:15:12 **22** numerous terrorist attacks, namely vehicle-borne improvised
00:15:17 **23** explosive device (VBIED) attacks, aimed to topple the Saudi
00:15:23 **24** Arabian government in hopes of establishing a new government
-08:-44:-46 **25** that would not ally itself with the United States. The group's

-08:-44:-46 **1** claimed attacks have included the killing of dozens of lives --
-08:-44:-46 **2** I assume persons -- including Americans.

00:15:36 **3** I'm going to make that correction.

00:15:46 **4** Ansar Al Sunnah: Group of armed Sunni Iraqi
-08:-44:-46 **5** terrorists that operate primarily in northern and central Iraq.

00:15:57 **6** Bashmirqah or Pesh Merga: Armed militia who have
00:16:05 **7** historically fought for the independence of the predominantly
00:16:09 **8** populated Kurdish area of northern Iraq.

00:16:12 **9** Iraqi Resistance Islamic Front: An Iraqi group
-08:-44:-46 **10** that announced its creation in 2004 that unified several smaller
-08:-44:-46 **11** Sunni groups that have used terrorist tactics and attacks
00:16:25 **12** against Coalition Forces.

00:16:26 **13** Islamic Army of Iraq (IAI): A group formed in or
-08:-44:-46 **14** around 2003 that focuses on committing terrorist attacks in
-08:-44:-46 **15** Iraq's Western province of Al-Anbar.

00:16:39 **16** Mossad: Institute for intelligence and special
-08:-44:-46 **17** operations; it is the national intelligence agency for the State
00:16:50 **18** of Israel.

-08:-44:-46 **19** Muslim brotherhood (Ikhwan Muslimeen): An Egyptian
00:16:58 **20** political opposition group formed in 1928 by Hasan al-Bana whose
00:17:03 **21** platform claims to be based on Islamic law.

00:17:06 **22** Taliban: Political and religious terrorist militia
-08:-44:-46 **23** and faction that came to power in Afghanistan in the mid 1990s.
-08:-44:-46 **24** The Taliban allowed Afghanistan to serve as a haven for Al
00:17:22 **25** Qaeda.

00:17:22 **1** Hamas: An organization designated by the U.S. as a
-08:-44:-46 **2** foreign terrorist organization (FTO).

00:17:30 **3** Hizballah, also spelled Hezbollah, I think. There
-08:-44:-46 **4** are various spellings. Hizballah: An organization designated
-08:-44:-46 **5** by the U.S. as a foreign terrorist organization (FTO).

00:17:48 **6** The next category consists of individuals.

00:17:53 **7** Al Albany, Muhamma Nasiruddin: An Islamic scholar
-08:-44:-46 **8** of the 20th century.

00:18:05 **9** Al Ayyiri, Yousef: Author of Al Qaeda publications
00:18:08 **10** that announced the group's strategy in combat by "expanding the
-08:-44:-46 **11** battlefield and exhausting the enemy."

00:18:15 **12** Al Dosari, Abul-Harith Abdelrahman: Suicide bomber
-08:-44:-46 **13** depicted in the "Winds of Victory" as carrying out the martyrdom
00:18:28 **14** operation at the Khalidiyah Bridge.

-08:-44:-46 **15** MR. TERESINSKI: Your Honor, they're listed by the
00:18:33 **16** last name first. So if you want to go first name then last
-08:-44:-46 **17** name, that's fine.

00:18:38 **18** THE COURT: I'll read them as they are here.

00:18:41 **19** MR. TERESINSKI: That's fine.

-08:-44:-46 **20** THE COURT: The names are first name second.

00:18:49 **21** Thank you.

-08:-44:-46 **22** The Khalidiyah Bridge is in Baghdad?

00:18:57 **23** MR. TERESINSKI: I'm sorry.

-08:-44:-46 **24** THE COURT: The Khalidiyah Bridge is in what city?

-08:-44:-46 **25** Do we know? I think it's in Baghdad.

00:19:07 **1** MR. TERESINSKI: I think it's further defined.

00:19:10 **2** Al Ghamdi, Abu Al-Walid: The leader of the

00:19:16 **3** Mujahidin fighters in Chechnya in 2002.

00:19:19 **4** Al Muqrin, Abd Al Aziz: Former head of Al-Qaeda in

-08:44:-46 **5** the Arabian Peninsula.

00:19:33 **6** Al Shaalan, Hazim: Former Iraqi defense minister

-08:44:-46 **7** in the Interim Iraqi government from June of 2004 to January

00:19:41 **8** 2005.

00:19:42 **9** Al Shami, Abu Anas (also known as the Lion of

00:19:48 **10** Fortifications): Abu Musab al Zarqawi's deputy, reported to

-08:44:-46 **11** have been killed in 2004.

00:19:58 **12** Al Timimi, Ali: Prominent Muslim scholar who, in

00:20:04 **13** 2005, was found guilty of soliciting others to levy war against

-08:44:-46 **14** the United States and inducing others to use firearms in

00:20:13 **15** violation of federal law.

00:20:16 **16** Al Zawahiri, Ayman: An Egyptian who currently

-08:44:-46 **17** serves as second-in-command of Al-Qaeda. Zawahiri frequently

00:20:29 **18** delivers video and audio messages to U.S. and world audiences on

-08:44:-46 **19** behalf of Al-Qaeda.

00:20:35 **20** Al Zarqawi, Abu Musab: A Jordanian who was the

-08:44:-46 **21** leader of Al-Qaeda in Iraq until he was killed in 2006.

00:20:46 **22** Al Hariri, Rafiq Bahaa El Deen: Prime Minister of

00:20:51 **23** Lebanon from 1992 to 1998, and 2000 to 2004. Al-Hariri was

00:20:58 **24** killed on February 14, 2005, when explosives were detonated near

-08:44:-46 **25** his motorcade in Beirut, Lebanon.

00:21:06 **1** Allawi, Ayad: Allawi was the Prime Minister of the
-08:44:-46 **2** Interim Government of Iraq.

00:21:14 **3** Atta, Mohamed: Egyptian; tactical leader of the
-08:44:-46 **4** September 11, 2001 plot; pilot/highjacker, American Airlines
-08:44:-46 **5** Flight 11 (Deceased).

00:21:26 **6** Azzam, Abdullah: A Palestinian who served as the
-08:44:-46 **7** intellectual mentor to Usama Bin Laden and was a leader of the
00:21:37 **8** mujahidin who traveled to Afghanistan in order to fight the
00:21:42 **9** Soviet Union in the 1980s. Azzam was killed in 1989.

00:21:48 **10** Basayev, Shamil: Chechen Islamic militant and
00:21:53 **11** leader of the Chechen separatist movement.

-08:44:-46 **12** Bigley, Kenneth: British engineer who was
00:22:01 **13** kidnapped and taken hostage in September 2004 before being
-08:44:-46 **14** beheaded by Al-Qaeda in Iraq.

00:22:06 **15** Bin Laden, Usama: A Saudi Arabian national who is
-08:44:-46 **16** the leader of a U.S.-designated terrorist organization called
-08:44:-46 **17** "Al-Qaeda".

00:22:18 **18** Chalabi, Ahmed: A Shi'a who founded the Iraqi
-08:44:-46 **19** National Congress (INC), a group of Iraqi exiles who sought the
00:22:30 **20** ouster of Saddam Hussein.

-08:44:-46 **21** Hekmatyar, Gulbuddin: Founder of the Islamic group,
00:22:37 **22** Hezb-i-Islami, which seeks the establishment of an Islamic
00:22:41 **23** republic in Afghanistan.

00:22:43 **24** Ibn Tamiyah: One of Islam's theologians from the
00:22:47 **25** early 1300s.

00:22:50 **1** Johnson, Paul Marshall: Was an American helicopter
00:22:55 **2** engineer who lived in Saudi Arabia. In 2004, he was taken
-08:-44:-46 **3** hostage by terrorists and beheaded on video tape.

-08:-44:-46 **4** Khattab, Omar Ibn: The Saudi-born leader of the
00:23:07 **5** Chechen mujahidin. Khattab died in 2002.

00:23:12 **6** King Fahd: The King of Saudi Arabia from 1982 to
00:23:17 **7** 2005.

00:23:19 **8** Mullah Mohammed Omar: Believed to be a Taliban
00:23:22 **9** leader who became the de facto leader of Afghanistan in 1996.

00:23:28 **10** Mullah Omar reportedly instituted strict Islamic law on the
00:23:32 **11** Afghan people. Al-Qaeda operated freely out of Afghanistan
-08:-44:-46 **12** during his rule.

00:23:37 **13** Sadat, Anwar: President of Egypt from 1970 until
-08:-44:-46 **14** his assassination in 1981.

-08:-44:-46 **15** Miscellaneous terms.

-08:-44:-46 **16** .50 caliber: A large caliber cartridge fired from
-08:-44:-46 **17** a variety of heavy machine guns, including weapons with a
00:23:56 **18** rotating or spinning barrel (also known as Gatling guns).

00:24:00 **19** Apostate: One who renounces or abandons a
00:24:05 **20** particular religious faith.

-08:-44:-46 **21** C4: A type of plastic explosive.

00:24:10 **22** Hown: Nickname of a Bosnian Mujahideen, Abu Abdel
00:24:17 **23** Azia "Barbaros", based on his proficiency in using Soviet-made
-08:-44:-46 **24** "Hound" artillery rockets.

-08:-44:-46 **25** Infidel: A derogatory term used to describe an

00:24:27 **1** unbeliever with respect to a particular religion. The term has
-08:-44:-46 **2** been used in this case to describe an unbeliever in the religion
-08:-44:-46 **3** of Islam.

00:24:35 **4** Jew's Mallow Soup: A common soup in the Middle
-08:-44:-46 **5** East made from molukhia (or Jew's mallow) which is a type of
-08:-44:-46 **6** green.

00:24:44 **7** Kalashnikov: Term for an AK-47, an automatic
-08:-44:-46 **8** rifle.

00:24:51 **9** Madrid Bombings/Atocha Train Station: A series of
00:24:57 **10** coordinated bombings against the commuter rail system of Madrid,
-08:-44:-46 **11** Spain, that took place on the morning of March 11, 2004, killing
00:25:07 **12** 191 people and wounding 1,755. Three bombs exploded in the
00:25:12 **13** Atocha station.

00:25:14 **14** M16: The M16 has been the primary infantry rifle
00:25:20 **15** of the United States military since the 1960s.

-08:-44:-46 **16** M203: A grenade launcher used by the United
00:25:30 **17** States military and some other countries.

00:25:32 **18** RPG (Rocket Propelled Grenade): A loose term
00:25:37 **19** describing hand-held, shoulder-launched antitank weapons capable
-08:-44:-46 **20** of firing an unguided rocket equipped with an explosive warhead.

-08:-44:-46 **21** USS Cole: U.S. naval vessel attacked by Al-Qaeda
-08:-44:-46 **22** suicide bombings operatives in the Port of Aden, Yemen, in 2000.

00:25:58 **23** The Cole was damaged and 17 U.S. sailors were killed in the
-08:-44:-46 **24** attack.

00:26:06 **25** Then, rather than rereading everything, the

00:26:09 1 definitions are repeated in the back. In other words, we've
00:26:12 2 provided them to you both topically and alphabetically. Okay.
00:26:19 3 So ready to call your next witness?
-08:-44:-46 4 MR. HERDMAN: Yes, Your Honor. United States of
00:26:23 5 America calls Joseph Corrigan. He is a computer forensic
-08:-44:-46 6 analyst for the FBI.
-08:-44:-46 7 THE COURT: While he comes in, I want to publicly
00:26:35 8 acknowledge the work and the cooperative work between counsel in
-08:-44:-46 9 this case that has enabled me to give you these definitions. I
-08:-44:-46 10 think that it shows a willingness on the part of all counsel,
-08:-44:-46 11 which is most commendable, to see to it that you, as fully as
-08:-44:-46 12 possible, understand everything having to do with this case.
00:26:57 13 Thank you. Okay.
00:27:24 14 (The witness was sworn by the clerk.)
00:27:29 15 THE COURT: Take a seat. You have to get about
-08:-44:-46 16 this distance from the microphone. Much closer, we get
-08:-44:-46 17 feedback; further away, we don't hear you. So even though I'm
-08:-44:-46 18 addressing you, you can turn to the jury and speak to them
-08:-44:-46 19 because it is they who have to hear your various answers.
00:27:58 20 Will you tell me and the ladies and gentlemen of
-08:-44:-46 21 the jury your name, and spell your name?
00:28:01 22 THE WITNESS: My name is Joe Corrigan,
-08:-44:-46 23 C-o-r-r-i-g-a-n.
00:28:06 24 THE COURT: Mr. Corrigan, do you have an occupation
-08:-44:-46 25 or profession?

00:28:22 1 THE WITNESS: Yes. I am an information technology
00:28:25 2 specialist, forensic examiner for the Federal Bureau of
00:28:29 3 Investigation.

00:28:31 4 THE COURT: And where are you stationed? What's
-08:44:46 5 your duty station?

00:28:36 6 THE WITNESS: Cleveland.

-08:44:46 7 THE COURT: How long have you worked for the FBI?

00:28:40 8 THE WITNESS: Approximately four years.

00:28:43 9 THE COURT: What do you do for the FBI? Just
-08:44:46 10 generally, just one paragraph of less job description, if you
-08:44:46 11 can.

00:28:50 12 THE WITNESS: Computer forensics for the FBI.
-08:44:46 13 What that is, whenever you hear that they take computers on a
-08:44:46 14 case, I'm the guy that actually goes into the computers looking
-08:44:46 15 for evidence.

00:29:05 16 THE COURT: How do you do that? Just generally
-08:44:46 17 again. There may be more questions about it. Just generally,
00:29:14 18 sort of how do you do your job?

00:29:16 19 THE WITNESS: Basically what I do is I take the
00:29:21 20 computer or CD; I make an exact duplicate of that CD or computer
00:29:26 21 hard drive. Then I work from a copy of that using forensic
00:29:30 22 tools.

00:29:32 23 THE COURT: Before going to work for the FBI,
-08:44:46 24 perhaps starting with college -- did you go to college?

00:29:40 25 THE WITNESS: Yes, I did.

00:29:41 **1** THE COURT: And when and where did you graduate?

00:29:43 **2** THE WITNESS: I graduated from Bluffton College in

-08:44:-46 **3** the year 2001.

00:29:50 **4** THE COURT: What was your major?

-08:44:-46 **5** THE WITNESS: Computer science.

-08:44:-46 **6** THE COURT: Then what did you do between then and

-08:44:-46 **7** going to work for the Bureau?

00:29:57 **8** THE WITNESS: Prior to the Bureau service, I worked

-08:44:-46 **9** for General Electric in Cleveland, Ohio, for just about six

-08:44:-46 **10** months. And then I went to work for the Attorney General of

00:30:09 **11** Ohio's office under the Bureau of Criminal Investigation from

00:30:15 **12** 2001 until 2005.

00:30:18 **13** THE COURT: And what did you do for GE and what did

-08:44:-46 **14** you do for the Bureau of Criminal Investigation?

-08:44:-46 **15** THE WITNESS: For GE I was a UNIX technical

-08:44:-46 **16** analyst. UNIX is an operating system like Microsoft system is

-08:44:-46 **17** an operating system. They have a bunch of computers at GE. I

-08:44:-46 **18** maintained them. And when something broke on them, I replaced

00:30:44 **19** hardware or sometimes -- or something with software, I would fix

00:30:50 **20** it.

-08:44:-46 **21** Then for BCI, what I did, the same thing I do for

-08:44:-46 **22** the FBI, was computer forensics.

-08:44:-46 **23** THE COURT: Okay. Mr. Herdman, you may inquire.

00:31:02 **24** MR. HERDMAN: Thank you, Your Honor.

00:31:03 **25** - - -

00:31:03 1 JOSEPH CORRIGAN, DIRECT EXAMINATION

-08:44:46 2 BY MR. HERDMAN:

-08:44:46 3 Q. Good morning, Mr. Corrigan. You talked a little bit

-08:44:46 4 about your educational background at Bluffton College. You

-08:44:46 5 said you got a BA in Computer Science?

-08:44:46 6 A. That's correct.

-08:44:46 7 Q. While you were actually in college at Bluffton, did you

00:31:16 8 work at all while you were in college?

-08:44:46 9 A. Yeah. I had -- my first job was working for the

00:31:23 10 Cleveland Indians Baseball Club working in the merchandising

-08:44:46 11 department where I sold merchandise as well as did some general

00:31:36 12 desktop support. So when someone's computer broke, I would fix

00:31:41 13 it, or when they had general computer questions.

-08:44:46 14 Q. Did you also work at GE while you were a student?

00:31:48 15 A. I did my internship at General Electric. After I

00:31:52 16 graduated in 2001, I got my first full-time job there.

-08:44:46 17 Q. Then after you graduated from Bluffton, you worked for

00:31:58 18 GE for about six months?

-08:44:46 19 A. That's correct.

00:32:01 20 Q. Then you were hired by the Ohio Bureau of Criminal

-08:44:46 21 Investigation?

00:32:04 22 A. That's correct.

-08:44:46 23 Q. What initials does that go by?

-08:44:46 24 A. BCI.

-08:44:46 25 Q. What is BCI? Can you just explain that to the jury?

-08:44:46 1 A. BCI provides local law enforcement assistance in cases
-08:44:46 2 that are either complex or unusual.

00:32:19 3 Q. And what -- you said you were a computer forensic
-08:44:46 4 specialist for the Ohio BCI as well?

-08:44:46 5 A. That is correct.

00:32:25 6 Q. What kind of training did you have to receive in order
00:32:30 7 to work for Ohio BCI as a computer forensic examiner?

-08:44:46 8 A. The first was an initial six months at BCI's
00:32:39 9 headquarters in London, Ohio, where I was down there learning
-08:44:46 10 from other people in the computer lab. I attended lots of
00:32:53 11 classes through various organizations such as HTCLA, which is
-08:44:46 12 the High Tech Criminal Investigation Association. And I also
00:33:04 13 obtained certifications from an organization called IACIS, which
-08:44:46 14 is the International Association of Computer Investigative
00:33:15 15 Specialists. One was certified electronic evidence collection,
00:33:23 16 and then the other one was certified forensic computer examiner.

-08:44:46 17 Q. I'm going to ask you to pull up Exhibit 166. Do you
-08:44:46 18 recognize that, Mr. Corrigan?

-08:44:46 19 A. Yeah. That's my curriculum vitae.

00:33:57 20 Q. If we could go to the second page. Here it's really
-08:44:46 21 kind of small. Here's -- this is a listing of your
00:34:09 22 certifications and training. Can you pick out a couple of the
-08:44:46 23 highlights off of this for the jury?

00:34:16 24 A. Like I mentioned before, I obtained my certified
00:34:20 25 forensic computer examiner from IACIS in 2002. I also am

-08:-44:-46 1 certified through the FBI to work on computer cases as well as
00:34:33 2 do investigations on PDAs, which are personal data assistants,
-08:-44:-46 3 like hand-held calendars and that kind of stuff, as well as cell
-08:-44:-46 4 phones. And then Linux, which is kind of like UNIX, it's an
00:34:54 5 operating system, something that Microsoft uses.

00:35:01 6 Q. Touch your screen. See if you can highlight the August
00:35:05 7 15, 2002 IACIS certification.

00:35:05 8 A. (Complied.)

00:35:10 9 Q. Now, that's got one date on it, August 15, 2002. But
-08:-44:-46 10 can you explain for the jury what the process was leading up to
00:35:17 11 that certification?

-08:-44:-46 12 A. In, I believe, April, 2002, I went to Florida to take
-08:-44:-46 13 this class. It's two weeks long. Then after the class is
00:35:32 14 done, they give you problems, an essay, an exam to write, and
-08:-44:-46 15 which you work on after the class. Then after you're done with
-08:-44:-46 16 it, you submit it for -- to see if you certify under their
00:35:46 17 program. And the final -- the day I sent it out was August 15.

-08:-44:-46 18 Q. Do you have to be recertified for that process?

-08:-44:-46 19 A. Yes.

00:35:54 20 Q. And I see on here that you were recertified at some
00:36:00 21 point in 2005?

-08:-44:-46 22 A. Correct.

-08:-44:-46 23 Q. December 1, 2005. Can you hit that for the jury.

-08:-44:-46 24 December 1, 2005.

-08:-44:-46 25 A. (Complied.)

00:36:13 **1** Q. Now, you testified that you went to go work for the FBI
-08:-44:-46 **2** after you worked for the BCI, correct?
-08:-44:-46 **3** A. Correct.
-08:-44:-46 **4** Q. How long did you work for BCI?
00:36:23 **5** A. BCI was four years.
-08:-44:-46 **6** Q. What kind of investigations did you work on at BCI?
00:36:29 **7** A. Boy, anything now could really be -- a computer could be
00:36:34 **8** involved in homicide investigations, drug investigations, child
00:36:42 **9** pornography investigations. Really anytime the person's using
00:36:47 **10** a computer to commit a crime, or perhaps doing some research on
-08:-44:-46 **11** how to commit a crime, or just who they talk to before a crime
00:37:00 **12** may have been committed would be relevant.
-08:-44:-46 **13** Q. So can you just explain for the jury, when you worked
-08:-44:-46 **14** for Ohio BCI, who was it you were providing assistance to in
00:37:12 **15** investigations?
-08:-44:-46 **16** A. Any local law enforcement from the State of Ohio. So
-08:-44:-46 **17** Toledo Police Department, for example, or Cleveland Police
-08:-44:-46 **18** Department, or sheriff's office as well.
00:37:23 **19** Q. And you worked at BCI until when?
-08:-44:-46 **20** A. Until 2005.
-08:-44:-46 **21** Q. And then that's when you went to go work for the FBI?
-08:-44:-46 **22** A. Correct.
-08:-44:-46 **23** Q. By the way, I notice on your qualifications or your
00:37:37 **24** certifications -- if you could zoom in on the bottom here, May
00:37:45 **25** 15, 2005 -- I notice here it says CART. I just hit it there

00:37:50 **1** and covered it up.

00:37:53 **2** Can you remind the jury what CART is? I think
-08:44:46 **3** they've heard it before.

-08:44:46 **4** A. CART is Computer Analysis Response Team.

00:37:59 **5** Q. Is that something that the FBI uses, a term they use?

-08:44:46 **6** A. Yes. It's FBI terminology.

-08:44:46 **7** Q. When you went to go work for the FBI, were you assigned
00:38:07 **8** in some way to CART?

-08:44:46 **9** A. Yes.

00:38:11 **10** Q. Did you have to undergo a separate training program when
-08:44:46 **11** you went to go work for the FBI?

-08:44:46 **12** A. Yes, I did.

00:38:17 **13** Q. And can you just describe briefly what that training
-08:44:46 **14** process was like?

-08:44:46 **15** A. I was able to test out of a lot of the stuff that you'd
00:38:27 **16** normally have to go through just because I'd already been
-08:44:46 **17** working on computer forensics prior to me joining the Bureau.
00:38:35 **18** But it's just a series of courses and take-home exams certifying
00:38:41 **19** you to -- you to conduct examinations for the FBI.

00:38:46 **20** Q. And I see here that -- I think you said this before, but
00:38:50 **21** just to point out your CART certifications, can you go through
-08:44:46 **22** those really quickly?

-08:44:46 **23** A. Certified to work on PDAs, cell phones, just regular
00:39:00 **24** computers and computers with Linux operating system.

-08:44:46 **25** Q. Have you ever served as an instructor for any law

00:39:10 **1** enforcement organizations or schools?

00:39:12 **2** A. Yes, I've instructed at the Ohio Peace Officer Training

00:39:26 **3** Academy in their data recovery classes and internet

00:39:30 **4** investigations and first responder classes, as well as HTCLA,

00:39:40 **5** teaching a course of Linux forensics.

-08:-44:-46 **6** Q. Have you ever been qualified in court to render

00:39:48 **7** evidence?

-08:-44:-46 **8** A. Yes, I have.

-08:-44:-46 **9** Q. Have you done that in Ohio state court?

00:39:51 **10** A. Yes.

-08:-44:-46 **11** Q. Was that about six times you were qualified?

-08:-44:-46 **12** A. Correct.

-08:-44:-46 **13** Q. What about in this federal court, have you ever been

-08:-44:-46 **14** qualified to render opinion evidence?

-08:-44:-46 **15** A. Yes.

00:40:00 **16** Q. Do you remember the name of that case?

00:40:03 **17** A. U.S. versus Monea, M-o-n-e-a, I think. That was in

-08:-44:-46 **18** Akron, Ohio.

00:40:12 **19** MR. HERDMAN: At this time I would move to qualify

-08:-44:-46 **20** Joe Corrigan as an expert able to render opinion testimony on

-08:-44:-46 **21** computers and analysis.

00:40:24 **22** MR. HARTMAN: No objection.

00:40:28 **23** MR. BRYAN: No objection.

00:40:30 **24** THE COURT: Do you recall the nature of that case,

-08:-44:-46 **25** the federal case in Akron?

00:40:35 1 THE WITNESS: I believe it was an embezzling case
-08:44:46 2 where an attorney was embezzling, I think, \$2 million or
-08:44:46 3 something.

00:40:44 4 THE COURT: Okay. Go ahead. That was an Akron
00:40:56 5 attorney?

00:40:57 6 MR. HARTMAN: Nobody in this room?

00:41:01 7 THE COURT: Go ahead, Mr. Herdman.

-08:44:46 8 MR. HERDMAN: Thank you, Your Honor.

-08:44:46 9 BY MR. HERDMAN:

00:41:06 10 Q. The Judge asked you before just sort of to generally
-08:44:46 11 explain what it is you do. When you're conducting a forensic
-08:44:46 12 examination of a piece of evidence, whether a computer or cell
-08:44:46 13 phone, what is the first step that you do?

-08:44:46 14 A. What I do is I check out the computer or the discs from
-08:44:46 15 evidence control, and I do an initial physical examination where
-08:44:46 16 I write down the serial number of the hard drive. Then what I
-08:44:46 17 do is make an exact duplicate of that hard drive. After it's
-08:44:46 18 done making a duplicate, I verify that nothing -- that it is, in
-08:44:46 19 fact, an exact duplicate and nothing had changed from the
-08:44:46 20 original. After the original is done, I check it back into
-08:44:46 21 evidence and do all my examination on the copy.

00:42:03 22 Q. Why is it you do your examination on the copy of
-08:44:46 23 whatever the piece of evidence is?

-08:44:46 24 A. It's just a safeguard to -- in case something were to go
-08:44:46 25 wrong that I would not be altering original evidence. It would

00:42:16 **1** just be a copy of that.

-08:44:46 **2** Q. What would be the reason that you wouldn't just take,

00:42:23 **3** say, a computer and turn it on and start going through the

00:42:26 **4** computer to see what's on that computer?

00:42:28 **5** A. Because that's going to be changing the evidence. It's

-08:44:46 **6** going to be adding files. As soon as you turn it on, Windows

00:42:35 **7** is going to start changing the files, it's accessing system

00:42:40 **8** files, it's loading your desktop, and it's going to change the

-08:44:46 **9** dates that are on the computer.

-08:44:46 **10** Q. So if I just turn on a computer and I don't touch

-08:44:46 **11** anything, it's going to change the computer itself?

-08:44:46 **12** A. Correct.

00:42:53 **13** Q. And that's why you make a copy of that computer?

-08:44:46 **14** A. Yes.

-08:44:46 **15** Q. Now, what steps do you go through in order to examine or

00:42:59 **16** analyze that forensic evidence that you've obtained from the

00:43:05 **17** computer?

-08:44:46 **18** A. It depends on what was submitted. For hard drives, what

-08:44:46 **19** we'll do is we'll put it into forensic software called Access

00:43:16 **20** Data Forensic Toolkit. What that is --

-08:44:46 **21** Q. Do you refer to Forensic Toolkit by an acronym?

-08:44:46 **22** A. FTK.

00:43:26 **23** What that program does is it takes the copy of that

-08:44:46 **24** hard drive and it categorizes everything. So it scans it and

-08:44:46 **25** it sees a word in a document, so it puts it in the document

-08:44:46 1 folder. It sees pictures, puts it in a folder. Just a way to
-08:44:46 2 organize the computer so all common things are in one area. It
00:43:47 3 also remembers or records all the words in the documents. So
00:43:53 4 when you do searches, you type in a word, and it will say, okay,
-08:44:46 5 these files contain this word.

00:44:00 6 Q. Are you able to recover files that maybe the user of
-08:44:46 7 that computer thought were deleted or recycled in some way?

-08:44:46 8 A. Yes.

-08:44:46 9 Q. How is it that the software is able to recover that
00:44:12 10 material that the person who was using the computer thought was
00:44:16 11 deleted?

-08:44:46 12 A. Okay, if you think of a computer as the library, you go
-08:44:46 13 into the library and want to look up a book. You go to the
-08:44:46 14 card catalog, and the card catalog tells you, okay, that book is
-08:44:46 15 on shelf 23. If you think of that as a computer, and you want
-08:44:46 16 to access the file, the computer uses the card catalog to show
00:44:43 17 you where the data on that file is. When you delete a file
00:44:48 18 normally in Windows, what it does is it just throws that card
00:44:54 19 catalog entry out. So the book is still on the shelf; it's
-08:44:46 20 just the pointer to where that book is located has been removed.
00:45:03 21 It has -- it's kind of a little more involved than that in the
-08:44:46 22 fact that that space can be used by other files, so it can be
00:45:14 23 overwritten in time.

00:45:17 24 Q. Can a file -- let's stick with the book analogy for a
-08:44:46 25 second.

-08:44:46 1 Could part of the book be ripped out and remain on
-08:44:46 2 the shelf?

-08:44:46 3 A. Absolutely. It could be just a partial overwrite of
-08:44:46 4 the file, or it could be completely overwritten by another file.

00:45:35 5 Q. Getting back to the Forensic Toolkit software for just a
-08:44:46 6 second, how does that software recognize each individual file?

-08:44:46 7 Does it assign some sort of number?

00:45:49 8 A. Yeah. Every file that comes across, it assigns it a
00:45:55 9 unique number to that for identification purposes.

-08:44:46 10 Q. So even if you had five identical documents in a
-08:44:46 11 computer, all five of those identical documents, if they existed
-08:44:46 12 as separate files, they will all have a unique number?

-08:44:46 13 A. Yes, they will.

-08:44:46 14 Q. Does the Forensic Toolkit software have the ability to
00:46:12 15 read Arabic characters?

00:46:20 16 A. In the contents of files, yes. So if the Arabic
00:46:24 17 lettering is inside a file, then yes, it will be able to display
18 it. However, if the Arabic language is inside the file name,
-08:44:46 19 it assigns some random string of letters to that file name.

-08:44:46 20 Q. Are you able to preserve the original Arabic characters
-08:44:46 21 in a file name when you're reviewing evidence through the
00:46:47 22 Forensic Toolkit software?

-08:44:46 23 A. Yes, by using another tool that does not have that
00:46:52 24 limitation, I can preserve the file names so I can compare the
00:46:58 25 files that FTK saw to what another tool sees. Then when they

-08:44:46 1 match up, I can say that that file name is what FTK saw it as.

00:47:17 2 Q. I'm going to direct your attention to 165D-1.

00:47:29 3 Mr. Corrigan, do you recognize what's displayed on
-08:44:46 4 the monitor?

-08:44:46 5 A. Yes.

-08:44:46 6 Q. What is that?

-08:44:46 7 A. A portion of my report.

-08:44:46 8 Q. And I guess this is -- is this an example of what you
-08:44:46 9 were just trying to put into words?

-08:44:46 10 A. Absolutely. This is that unique item number showing

-08:44:46 11 what FTK assigns each file, then also what FTK assigned as the
-08:44:46 12 name of that file. And then using another program in the file

00:47:57 13 listings full pad I exported the correct, for lack of a better

-08:44:46 14 word, representation of the file name. And then where those

-08:44:46 15 files matched exactly, I associated that name to what FTK called
-08:44:46 16 it.

00:48:22 17 Q. Would you go to page 50, please. And I'd like to

00:48:28 18 direct your attention to maybe this one here.

00:48:28 19 A. (Complied)

00:48:33 20 Q. That first column you said was the FTK number that's
-08:44:46 21 assigned?

00:48:37 22 A. That is correct.

00:48:38 23 Q. And then the FTK software assigns the name that's in
-08:44:46 24 this part right here, correct?

-08:44:46 25 A. Yes.

-08:44:46 1 Q. Can you tell by looking at that -- if you didn't have
-08:44:46 2 the right column here, can you tell by looking at what's in the
-08:44:46 3 second column that there was an Arabic file name in that file?

00:48:59 4 A. In the first column?

00:49:07 5 Q. In the column here where I've underlined in green, can
-08:44:46 6 you tell there's an Arabic file name if you just looked at this
00:49:16 7 in Forensic Toolkit?

-08:44:46 8 A. I assumed it. The coding or the format would not have
00:49:24 9 been just that seemingly random set of letters; it would
00:49:32 10 actually add a different name.

-08:44:46 11 Q. Then you were able --

-08:44:46 12 THE COURT: I'm sorry; I couldn't hear you.

00:49:38 13 THE WITNESS: The file would not have had that
00:49:41 14 seemingly random string of letters as the file name. It would,
00:49:46 15 in fact, be encoded using another language.

00:49:50 16 BY MR. HERDMAN:

00:49:50 17 Q. And then this third column, what does that third column
-08:44:46 18 show if we go across from this particular FTK number?

-08:44:46 19 A. The third column shows, using another tool, what the
-08:44:46 20 coding in Arabic would be.

00:50:07 21 Q. So what's in the right, the far right-hand column, is
-08:44:46 22 the Arabic file name as it would have appeared on any given
00:50:16 23 piece of computer evidence?

-08:44:46 24 A. Correct.

00:50:18 25 Q. And what's in the second column is the way the software

00:50:22 1 views it?

00:50:23 2 A. Right. Due to that limitation of the program.

-08:44:-46 3 Q. And then this document here, which is 165D-1, has

-08:44:-46 4 essentially preserved all of those original Arabic file names?

-08:44:-46 5 A. Yes.

00:50:37 6 Q. Now, when you conduct a forensic examination of computer

-08:44:-46 7 evidence, what kind of guidance do you receive from the case

00:50:46 8 agents?

00:50:47 9 A. Usually it is what they're looking for in the case;

00:50:53 10 sometimes it is dates that they're interested in; sometimes it's

00:51:01 11 types of files that they're interested in.

-08:44:-46 12 Q. Why is it that you rely on case agents to provide you

-08:44:-46 13 with certain information that's relevant to your forensic

-08:44:-46 14 examination?

00:51:10 15 A. Because they know the case a lot better than I do.

00:51:16 16 They know what they're looking for and what they're authorized

-08:44:-46 17 to search for.

-08:44:-46 18 Q. I'd like to ask you a couple sort of general computer

00:51:24 19 concepts that have already come up in the course of the case or

-08:44:-46 20 will come up in your testimony, and just ask you to describe

00:51:30 21 them, sort of in laymen's terms, for the jury if you can.

00:51:34 22 When we talk about a computer file, what is it that

-08:44:-46 23 we're talking about when we use the word "file"?

00:51:40 24 A. File is a way to organize information. It's like you

-08:44:-46 25 would print out a sheet of paper, and you want -- like my CV,

00:51:51 1 for example; I would want just my CV in one area. The file is
-08:44:46 2 a way to segregate just the data you want.

-08:44:46 3 Q. What is a directory?

-08:44:46 4 A. Directory is a way to organize files. So if you have,
-08:44:46 5 say, music on your computer, and you wanted to organize those
00:52:11 6 files into your favorite artists or albums, it's just a way of
00:52:16 7 organizing the data.

-08:44:46 8 Q. And files generally have extensions?

-08:44:46 9 A. Correct.

-08:44:46 10 Q. What is a file extension?

-08:44:46 11 A. File extension is a way to tell the operating system
00:52:29 12 what program opens this. So if you have, like, a .doc
-08:44:46 13 extension, that tells the computer that this is a Microsoft Word
-08:44:46 14 document. Or .jpg would be the JPEG, which is a bracket that
-08:44:46 15 tells the graphics, which tells the computer to open this with a
00:52:52 16 graphic viewer.

00:52:54 17 Q. What about the concept of burning a CD; what does that
00:52:57 18 mean?

-08:44:46 19 A. Burning a CD is just placing files from a hard drive
00:53:04 20 onto a CD for archiving purposes.

00:53:09 21 Q. And what about an MD5 hash number; what is that?

-08:44:46 22 A. When I said earlier when I compared the original to the
00:53:20 23 duplicate to make sure they were exactly the same, that is using
-08:44:46 24 an MD5 hash. Now, an MD5 hash can be considered like a
00:53:30 25 fingerprint for a file. Each file has a very unique

00:53:33 1 fingerprint. And this MD5 hash is that fingerprint. So I
00:53:38 2 compare the hash of my copy to the original. When they match,
-08:-44:-46 3 I know that it is an exact duplicate.

00:53:46 4 Q. So if -- let's use your CV example, your resumé. If
-08:-44:-46 5 you had a version up and you went in and you changed just a word
-08:-44:-46 6 in there, would that change the MD5 hash number of that
-08:-44:-46 7 document?

00:54:01 8 A. Absolutely. Even if you changed a capital P to a
-08:-44:-46 9 little P, it would completely change the fingerprint.

00:54:08 10 Q. I'd like to direct your attention to the forensic
00:54:12 11 examination and analysis you conducted in this case. You did
-08:-44:-46 12 perform a forensic examination and analysis of the computer
00:54:19 13 evidence in this case?

-08:-44:-46 14 A. Yes, I did.

00:54:21 15 Q. And what was the process that you went through to
-08:-44:-46 16 conduct that particular examination?

-08:-44:-46 17 A. In this case I collected all the evidence, imaged it,
-08:-44:-46 18 like I said, and then I set it up for the case agents to come
-08:-44:-46 19 and review. In this type of case it's a lot easier for me to
-08:-44:-46 20 work with the case agents a lot more than I usually do because
-08:-44:-46 21 they know what's relevant and what they're interested in.

00:54:51 22 Q. And did you complete a report at some point in this
-08:-44:-46 23 case?

-08:-44:-46 24 A. Yes, I did.

-08:-44:-46 25 Q. Was a portion of that a written report?

00:54:59 **1** A. Yes, it was.

00:55:00 **2** Q. Where would you say that the bulk of your report
00:55:03 **3** actually rested though, in the CDs?

00:55:06 **4** A. For me it would be the electronic evidence that I
-08:44:46 **5** exported.

00:55:18 **6** Q. Showing you what's been marked 165A, 165B, 165C and
-08:44:46 **7** 165D.

00:55:54 **8** MR. HERDMAN: May I approach the witness, Your
00:55:56 **9** Honor?

00:55:56 **10** THE COURT: Of course.

00:55:57 **11** BY MR. HERDMAN:

00:55:57 **12** Q. Take a look at those, Mr. Corrigan.

00:56:11 **13** The information that's contained on those CDs, is
-08:44:46 **14** that derived from the computer evidence in this case?

-08:44:46 **15** A. Yes, it is.

00:56:20 **16** MR. HERDMAN: Your Honor, at this point in time I'd
00:56:22 **17** offer Exhibits 165A, -B, -C, and -D into evidence.

00:56:27 **18** THE COURT: They'll be admitted.

00:56:29 **19** BY MR. HERDMAN:

-08:44:46 **20** Q. Now, Mr. Corrigan, since completing that report, have
-08:44:46 **21** you also provided information on two additional compact discs?

-08:44:46 **22** A. Yes, I have.

00:57:21 **23** MR. HERDMAN: Your Honor, may I approach the
-08:44:46 **24** witness?

-08:44:46 **25** THE COURT: Of course.

00:57:24 **1** BY MR. HERDMAN:

-08:44:46 **2** Q. Showing you 165E and 165F, can you take a look at 165E,

00:57:32 **3** Mr. Corrigan? What's actually on that particular CD?

00:57:36 **4** A. It is the information for, like, the locations of the

-08:44:46 **5** file to create modified access dates for the CDs I had made.

-08:44:46 **6** Q. We'll get to those in a little bit. What about 165F?

00:57:55 **7** A. It's the Real Player history for the cases 69440.

00:58:04 **8** Q. Is there information on two additional files on that

-08:44:46 **9** disc as well?

-08:44:46 **10** A. Yes.

00:58:08 **11** Q. And on those two CDs, 165E and -F, is the information

00:58:13 **12** that's contained on those CDs, is that also derived from the

00:58:17 **13** computer evidence in this case?

-08:44:46 **14** A. Yes, it is.

00:58:20 **15** MR. HERDMAN: I'd offer 165E and 165F into evidence

-08:44:46 **16** as well.

-08:44:46 **17** THE COURT: There being no objection, they'll be

00:58:27 **18** admitted.

00:58:28 **19** BY MR. HERDMAN:

00:58:28 **20** Q. With respect to the Arabic file, I know we talked about

-08:44:46 **21** this, but if you could bring up 165D-1.

-08:44:46 **22** You were able to preserve the original Arabic file

-08:44:46 **23** names of all the files that appear in your report?

-08:44:46 **24** A. That is correct.

00:58:44 **25** Q. And those are all listed here, 165D-1?

-08:44:46 **1** A. Yes.

-08:44:46 **2** Q. I'd like to direct your attention to Exhibit 61. Are
-08:44:46 **3** you familiar with this particular string of characters here?

00:59:18 **4** A. Yeah, it was identified to me by the case agent as being
00:59:22 **5** relevant in this case.

00:59:24 **6** Q. And these numbers at the bottom, the way that they're
-08:44:46 **7** written or set up, what do they indicate to you?

00:59:31 **8** A. It's an internet address, or URL.

00:59:36 **9** Q. Can you explain for the jury what an IP address is?

-08:44:46 **10** A. Right. IP address is kind of like your phone number.

-08:44:46 **11** It's a way of knowing how to get in contact with the
00:59:51 **12** information. When you go into your computer and you go onto
-08:44:46 **13** the internet, when you type in Google.com, what it's doing is
-08:44:46 **14** your computer is now asking your internet service provider, AOL
01:00:08 **15** or Roadrunner, whatever you have, where is Google.com located?
01:00:15 **16** And it comes back with this IP address or these numbers
-08:44:46 **17** separated by periods saying this computer's address has
01:00:25 **18** Google.com. So your computer contacts that and Google.com's
01:00:31 **19** home page appears to you.

-08:44:46 **20** Q. So what if I went into, say, my Internet Explorer, and I
01:00:37 **21** just typed in www.Google.com; am I typing in an IP address?

01:00:45 **22** A. You're typing in a domain name which your computer then
01:00:50 **23** translates into an IP address.

-08:44:46 **24** Q. What's the difference between an IP address and URL? I
-08:44:46 **25** heard you use that term.

-08:-44:-46 **1** A. IP address is URL. It's a Uniform Resource Locator or
01:01:02 **2** way to -- as well as domain name and IP address are URLs.
01:01:09 **3** Q. And this string of characters here, what is that? Is
-08:-44:-46 **4** that an IP address? Is that a URL? Is that a domain name?
01:01:17 **5** A. Those are folders on that server where the IP address
-08:-44:-46 **6** is.
01:01:24 **7** Q. How do you know that?
01:01:25 **8** A. "/VB" would be a folder.
-08:-44:-46 **9** Q. This part here?
-08:-44:-46 **10** A. Yes. Then "show thread PHP." PHP, without getting
-08:-44:-46 **11** too technical, is a way -- it's kind of like an HTML page, but
-08:-44:-46 **12** it's able to interact with the server more so it can pull data
01:01:49 **13** off the server.
01:01:51 **14** Q. One question. What's HTML?
01:01:54 **15** A. HTML is just the standard web page. When you go to
01:02:00 **16** Google.com and the search box appears and the graphic on the top
01:02:04 **17** appears, that is contained -- what's called data HTML file.
01:02:11 **18** Q. Are there different ways to view an HTML file?
01:02:14 **19** A. Yes.
-08:-44:-46 **20** Q. What are the different programs you could use to view an
01:02:17 **21** HTML?
-08:-44:-46 **22** A. You could use Explorer. Mozilla makes one called
-08:-44:-46 **23** Firefox.
-08:-44:-46 **24** Q. Can you spell that?
-08:-44:-46 **25** A. M-o-z-i-l-l-a. There's also various other internet

01:02:34 **1** browsers out there.

-08:-44:-46 **2** Q. Directing your attention back to what's on the screen

-08:-44:-46 **3** here, this part that says "show thread," and then there's the

-08:-44:-46 **4** letter "T=7821". What does that string of characters there tell

01:02:50 **5** you about perhaps the nature of this particular website?

01:02:54 **6** A. Commonly "VB" is virtual billboard or virtual bulletin

-08:-44:-46 **7** board. The "show thread" would be a thread in that bulletin

01:03:06 **8** board. A thread is kind of like a posting. So if you are

01:03:12 **9** familiar with -- if you have a phone book, for example, you

-08:-44:-46 **10** could go and pull up the different postings that companies have,

-08:-44:-46 **11** that they have an address, or it's just a way of identifying

01:03:30 **12** what resource you want to pull up. And that 7821 is just the

-08:-44:-46 **13** IP number of one particular posting.

01:03:39 **14** Q. On a virtual bulletin board when somebody posts

-08:-44:-46 **15** something generally, when somebody posts something, does it

01:03:46 **16** provide an opportunity for other people to go in and reply to a

01:03:49 **17** posting?

-08:-44:-46 **18** A. Absolutely.

01:03:58 **19** Q. Now, you discussed earlier that you used Forensic

01:04:04 **20** Toolkit software; you used it in examining computer evidence in

-08:-44:-46 **21** this case?

01:04:09 **22** A. Yes.

-08:-44:-46 **23** Q. Is that Forensic Toolkit software capable of searching

-08:-44:-46 **24** by an IP address?

-08:-44:-46 **25** A. Yes, I can enter that in the search.

-08:44:46 **1** Q. What about for a URL; could it do that as well?

01:04:20 **2** A. Absolutely. I can search pretty much any text stream I

01:04:26 **3** want.

-08:44:46 **4** Q. Did you conduct a search of this IP address or URL?

-08:44:46 **5** A. Yes, I did.

01:04:40 **6** Q. I'm going to show you Exhibit 165A-1.

-08:44:46 **7** Do you recognize this, Mr. Corrigan?

-08:44:46 **8** A. Yes, this is part of my report.

01:04:55 **9** Q. Now, if we could zoom in on the first part here,

01:05:04 **10** index.dat. Which computer does this relate to? Can you tell

-08:44:46 **11** by looking at it?

-08:44:46 **12** A. Yes. It is QV02 from the case 69440.

-08:44:46 **13** Q. Is that the same as Exhibit 76?

-08:44:46 **14** A. Yes, it is.

01:05:33 **15** Q. That's an HP Vectra desktop?

-08:44:46 **16** A. Correct.

01:05:39 **17** Q. Going back to the bookmarked page, if we zoom in on that

01:05:46 **18** first part there, what does this actually show you by looking at

01:05:51 **19** this?

-08:44:46 **20** A. This file I bookmarked was an internet history record.

-08:44:46 **21** So when you're using the Internet Explorer, it keeps track of

01:06:02 **22** the user name and where you visited on the internet and what

-08:44:46 **23** time it was when you did that by default. So this Internet

-08:44:46 **24** Explorer history record was the daily history for the day of

01:06:20 **25** 2005, February 6.

01:06:25 1 Q. What is that "created date" on the screen here? What
-08:44:46 2 does that indicate with respect to this particular file?
-08:44:46 3 A. With respect to this file, that's when the computer
01:06:36 4 created the data history file. So when it saw it was a new
-08:44:46 5 day, it created a few file. At the end of the week what
-08:44:46 6 typically happens is these daily history files are included into
-08:44:46 7 a weekly history file.

01:06:55 8 Q. Do you know whether there's some sort of a default
01:06:59 9 setting on Internet Explorer that would delete the internet
-08:44:46 10 history?

01:07:04 11 A. Right. After 20 -- I think the default is 21 days, but
-08:44:46 12 it's user configurable. You can set it to how long you want
-08:44:46 13 it to keep the history for.

-08:44:46 14 Q. Are you aware of whether the browser history for every
01:07:19 15 day, at least every day relevant to this case, was preserved in
-08:44:46 16 this Exhibit 76?

01:07:25 17 A. No, it is not.

-08:44:46 18 Q. What about prior to February 6? Let's say February 5,
-08:44:46 19 was the browser history for this particular computer, Exhibit
01:07:36 20 76, preserved?

-08:44:46 21 A. No, it's not.

-08:44:46 22 Q. What about, do you know if February 8 was preserved,
-08:44:46 23 that browser history?

-08:44:46 24 A. No.

-08:44:46 25 Q. February 16, was the browser's history preserved?

-08:-44:-46 1 A. I don't believe so.

-08:-44:-46 2 Q. Why would it be that the internet history browser
-08:-44:-46 3 history for February 6 was preserved whereas the day before it
01:07:58 4 wasn't preserved and a couple days after it wasn't preserved?

-08:-44:-46 5 A. That's a good question. It can be deleted by the user.

01:08:15 6 MR. HARTMAN: Objection, Your Honor. May we
01:08:17 7 approach?

-08:-44:-46 8 THE COURT: Sure.

01:08:18 9 (Whereupon the following discussion was had at the
01:10:11 10 bench outside the hearing of the jury:)

01:10:11 11 THE COURT: Your objection?

-08:-44:-46 12 MR. HARTMAN: I don't know if the government is
-08:-44:-46 13 going to different ways -- the reasons this could happen, but I
-08:-44:-46 14 don't want him to be speculating as to why, because he has no
-08:-44:-46 15 idea.

-08:-44:-46 16 THE COURT: I think the question is how. How
-08:-44:-46 17 could it be done technologically.

-08:-44:-46 18 MR. HARTMAN: Certainly if it calls for speculation
-08:-44:-46 19 in terms of opinion, I think that that particular witness has
-08:-44:-46 20 been qualified to render an opinion as to why or how this could
-08:-44:-46 21 be.

-08:-44:-46 22 THE COURT: How, I think. I realize there may be
-08:-44:-46 23 an overlap between how and why, but how can that be done. I
-08:-44:-46 24 thought that was the question.

-08:-44:-46 25 MR. HERDMAN: That's true.

-08:44:46 1 THE COURT: Why a particular individual might have
-08:44:46 2 done something --

-08:44:46 3 MR. HERDMAN: Honestly, Your Honor, there's not
-08:44:46 4 going to be any tie to any particular individuals here other
-08:44:46 5 than the computer.

-08:44:46 6 THE COURT: The impression I got from the question
-08:44:46 7 is how does one go about doing it.

-08:44:46 8 MR. HERDMAN: Yeah.

-08:44:46 9 MR. HARTMAN: The series of questions before that,
-08:44:46 10 just so I'm clear, 2/6 was preserved, but the other dates in
-08:44:46 11 February were not; is that what it was? I missed it.

-08:44:46 12 MR. HERDMAN: That was the string of questions,
-08:44:46 13 yes.

-08:44:46 14 (End of sidebar discussion.)

-08:44:46 15 THE COURT: Do you want to ask the question again?

01:10:19 16 MR. HERDMAN: I think I should, Your Honor.

01:10:23 17 BY MR. HERDMAN:

-08:44:46 18 Q. If we go back to this particular file here in the
-08:44:46 19 report, you indicated that this is the browser history for
-08:44:46 20 Exhibit 76, HP Vectra computer, for February 6, 2005?

-08:44:46 21 A. Correct.

01:10:40 22 Q. You just said that there wasn't a browser history for
01:10:44 23 February 5, 2005?

-08:44:46 24 A. Correct.

-08:44:46 25 Q. And there wasn't a browser history for, say, February 8,

-08:44:46 1 2005?

01:10:50 2 A. In this file, no.

01:10:53 3 Q. Why would -- or a better question is: How could a
-08:44:46 4 computer preserve the browser history for February 6 but not for
-08:44:46 5 February 5 or February 8?

-08:44:46 6 A. In this case, this file only contains one day's worth of
01:11:11 7 history, so it would just be for 2/6, 2005.

01:11:17 8 Q. Okay. Are you aware of whether or not this Exhibit 76,
-08:44:46 9 the computer that you examined in Exhibit 76, preserved the
-08:44:46 10 internet browser history for February 5, 2005?

01:11:29 11 A. It did not.

-08:44:46 12 Q. So I guess I'm talking outside of the context of this
01:11:34 13 particular file, when we're talking about the computer and the
01:11:37 14 computer preserving browser history, how is it that a computer
01:11:41 15 would preserve browser history for a particular date but not the
-08:44:46 16 date that preceded it or the date that was subsequent to it?

-08:44:46 17 A. It could be that the history was deleted. It could be
-08:44:46 18 that past the 21 days the computer automatically would delete
-08:44:46 19 that file to move it into a weekly history file, and then
01:12:06 20 subsequent, like I was saying before, that that file can be
-08:44:46 21 overwritten by another file, a new file that it's created.

-08:44:46 22 Q. So this particular file just may not have been
-08:44:46 23 overwritten yet?

01:12:19 24 A. Correct.

01:12:25 25 Q. If I could direct your attention to Exhibit 165A1-A, do

-08:-44:-46 1 you recognize this?

-08:-44:-46 2 A. Yes.

01:12:36 3 Q. What is this?

-08:-44:-46 4 A. This is a part of my report. What this is, FTK
01:12:43 5 interprets that internet history file, and this is its
01:12:47 6 interpretation of that.

01:12:49 7 THE COURT: Can you keep your voice up just a tad?

-08:-44:-46 8 I'm having a little trouble hearing you.

01:12:56 9 THE WITNESS: Okay.

01:12:59 10 MR. HERDMAN: If you go back to 165A-1.

01:13:08 11 BY MR. HERDMAN:

-08:-44:-46 12 Q. What we just saw on the screen, the browser history, is
-08:-44:-46 13 that the browser history that relates to Exhibit 76 here?

01:13:16 14 A. Yes, it is.

01:13:17 15 Q. For February 6, 2005?

01:13:19 16 A. Yes, it is.

01:13:21 17 MR. HERDMAN: You can go back to 165A1-A.

01:13:30 18 BY MR. HERDMAN:

-08:-44:-46 19 Q. So by looking at this browsing history, we can tell what
01:13:35 20 websites were accessed by Exhibit 76 on February 6, 2005?

01:13:41 21 A. Right. It's going to show you the daily internet
01:13:45 22 history file for 2/6, 2005, for the user name of Parent.

01:13:53 23 Q. If you can zoom in on that top box.

01:13:59 24 Maybe if you could go through, Mr. Corrigan, and
01:14:02 25 explain what each of these particular boxes mean. For example,

01:14:05 **1** URL, what does that mean?

-08:44:46 **2** A. URL, as shown before, is the address of the website.

-08:44:46 **3** The user name is the user name on the local computer of who
01:14:18 **4** visited that website. The last accessed date is when that was
01:14:24 **5** accessed, what the clock on the computer read, and UTC, or
01:14:31 **6** universal time coordinate.

01:14:40 **7** Q. The last access local?

-08:44:46 **8** A. Last access local. When Internet Explorer saves, it
01:14:47 **9** saves it in UTC time. What FTK does is it converts that to our
01:14:52 **10** local time. So that's what the time was in this eastern time.

-08:44:46 **11** Q. When this particular page was accessed by Exhibit 76?

-08:44:46 **12** A. Correct.

-08:44:46 **13** Q. Do you recognize that URL right there?

01:15:06 **14** A. Yes. It's the same one that was identified to me
-08:44:46 **15** earlier.

01:15:14 **16** Q. Do you know whether this daily browser history indicates
01:15:19 **17** that Exhibit 76, that HP Vectra computer, accessed that URL
-08:44:46 **18** 66.148 numerous times on February 6, 2005?

-08:44:46 **19** A. Yes.

01:15:33 **20** Q. I'd like to direct your attention to page 34 of this
-08:44:46 **21** exhibit, and the third box down. You see the same boxes there,
-08:44:46 **22** but in that URL can you explain for the jury what that URL
01:15:53 **23** string of characters indicates to you? What does that string of
-08:44:46 **24** characters indicate to you, Mr. Corrigan?

-08:44:46 **25** A. There's an area on the website called groups. It

01:16:15 **1** allows people to subscribe to them. There's groups for baseball
01:16:23 **2** clubs or football clubs or people who like dogs. It's just a
-08:44:-46 **3** way for people to kind of communicate with people that share a
-08:44:-46 **4** common interest usually. And in this URL it's showing that the
-08:44:-46 **5** e-mail address of Marwan El-Hindi at Yahoo.com was subscribing
-08:44:-46 **6** to a group named Arab_Times.

-08:44:-46 **7** Q. That was on February 6, 2005?

-08:44:-46 **8** A. Correct.

-08:44:-46 **9** Q. At about 4:00 p.m.?

01:16:58 **10** A. That is correct.

01:16:59 **11** Q. If I could direct your attention now to page 19 of this

01:17:04 **12** particular exhibit. And if you could go to that second block

-08:44:-46 **13** there. Again directing your attention to the URL, that string

-08:44:-46 **14** of characters there, can you explain for the jury what this

-08:44:-46 **15** particular URL indicates to you?

01:17:20 **16** A. Yahoo also has a feature where you can sign into the

01:17:25 **17** website using your Yahoo ID, so you can check your e-mail or

01:17:30 **18** look at the groups that you've joined or you can set up your

01:17:35 **19** favorite links. So what happened in this one was the login of

01:17:40 **20** Marwan El-Hindi logged into Yahoo at 2/6, 2005 at 10:05 p.m.

01:17:52 **21** Eastern.

-08:44:-46 **22** Q. It says password of -- p-a-s-s-w-d in the URL. That's

01:17:58 **23** in the second line from the bottom right there. Then there's a

-08:44:-46 **24** string of characters after that. What does that string of

01:18:08 **25** characters indicate to you?

01:18:09 1 A. That is the hash of his password. When I was talking
-08:44:46 2 about MD5 hash, internet sites also use hash as a way of
01:18:22 3 covering up a password. So when you type in your password --
01:18:27 4 say it's "dog". You type it in. It's not going to submit in
01:18:35 5 your URL: His password is dog. It's going to hash that so
-08:44:46 6 that rather than printing "dog", it prints the hash of it.
-08:44:46 7 Since it's unique, the hash is compared to whatever Yahoo
01:18:50 8 stores, then if that's correct, it logs him in.
-08:44:46 9 Q. That's so people can't get your password? It's a
-08:44:46 10 security function?
-08:44:46 11 A. It's just so if someone would look at the internet
01:19:01 12 history on your machine and they pulled that up, they wouldn't
-08:44:46 13 be able to see what you typed in. It would just be that
01:19:08 14 obfuscated hash.
-08:44:46 15 Q. So this particular part of your report indicates that
-08:44:46 16 someone logging in with the name Marwan El-Hindi and using a
-08:44:46 17 password logged into Yahoo.com on 2/6/05 at 10:05 p.m.?
-08:44:46 18 A. Correct.
-08:44:46 19 Q. If you could go to page 16. And then that first full
01:19:38 20 box up from the bottom. What does this particular part
01:19:49 21 indicate?
-08:44:46 22 A. It indicates the user name of Parent visited the URL at
01:19:54 23 2/6, 2005 at 10:18 p.m. Eastern.
-08:44:46 24 Q. 10:18. Okay.
01:20:03 25 MR. HARTMAN: I'm sorry, can we leave that up for a

01:20:06 1 second?

01:20:16 2 THE COURT: Is that the same page? I'm sorry.

-08:44:46 3 MR. HERDMAN: This is page 16, Your Honor.

01:20:22 4 THE COURT: Thanks.

01:20:28 5 MR. HARTMAN: Thanks.

01:20:30 6 MR. HERDMAN: Go to 3A.

01:20:44 7 BY MR. HERDMAN:

01:20:45 8 Q. That's Exhibit 3, Mr. Corrigan. Did you examine this

01:20:49 9 Dell laptop as part of your forensic examination as well?

-08:44:46 10 A. Yes, I did.

-08:44:46 11 Q. Were you able to determine whether this Dell laptop

01:20:56 12 accessed that IP address, 66.148, at any point during the

-08:44:46 13 investigation?

01:21:03 14 A. I don't recall.

01:21:06 15 MR. HARTMAN: I'm sorry. The answer?

01:21:10 16 THE WITNESS: I don't recall.

01:21:16 17 MR. HERDMAN: If we can go back to Exhibit 165A1.

01:21:16 18 BY MR. HERDMAN:

01:21:24 19 Q. If I could direct your attention to that second item.

01:21:28 20 What is that?

01:21:31 21 A. This is the internet history file for the username of

-08:44:46 22 Parent for cookies. Cookies are files that are placed on your

01:21:46 23 computer by a website in order to save information like the last

-08:44:46 24 time you visited. If you searched for Cleveland Indians

01:21:59 25 baseball scores one time, and you wanted every time you come to

-08:44:46 1 Yahoo.com sports page for the Cleveland Indians to come up, it

-08:44:46 2 will store just user preferences in there. It also can store

-08:44:46 3 your user name so you don't have to sign in every time. It's

01:22:17 4 just a way for the computer or the website to interact with the

01:22:22 5 user and then record some settings that the user sets.

01:22:27 6 Q. And how does the computer actually preserve a cookie?

-08:44:46 7 A. Cookies are contained in their own folder, and they have

-08:44:46 8 a history file associated with that folder.

-08:44:46 9 Q. And the actual cookie itself, what format is that cookie

-08:44:46 10 in?

01:22:50 11 A. Cookie is a text file.

-08:44:46 12 Q. If you look at that third item there on that page, is

-08:44:46 13 that an actual cookie?

-08:44:46 14 A. Yes.

-08:44:46 15 Q. You said it's a TXT file?

01:23:06 16 A. Correct.

01:23:07 17 Q. The second item you were talking about, this is actually

-08:44:46 18 a history of those cookies?

01:23:17 19 A. Correct. That is -- it records information about all

01:23:22 20 the cookies that are stored on there currently.

01:23:24 21 Q. And this again relates to Exhibit 76, the HP Vectra

01:23:31 22 computer?

-08:44:46 23 A. Correct.

01:23:34 24 Q. If we could pull up 165A1-B. Go to page 138. That

-08:44:46 25 second item, I guess it's the first full item on the page, I

-08:44:46 **1** direct your attention to that. What does this indicate to you,
-08:44:46 **2** Mr. Corrigan?

-08:44:46 **3** **A.** It's the internet history for that cookie. So it shows
-08:44:46 **4** that a cookie was placed on the computer by the website at
-08:44:46 **5** 66.148-85. The last time that that website accessed that cookie
-08:44:46 **6** was 4/2 of 2005. The last time it changed anything on that was
01:24:27 **7** 2/28 of 2005.

01:24:29 **8** **Q.** At least when we're talking about this cookie, what does
-08:44:46 **9** the access date indicate to you with respect to whether this
01:24:38 **10** particular computer actually went to that web page?

01:24:42 **11** **A.** That cookie -- that website interacted with that cookie.
01:24:47 **12** **Q.** And with respect to the last modified date, what does
-08:44:46 **13** that tell you with respect to this particular computer going to
-08:44:46 **14** this website?

01:24:55 **15** **A.** That was the last time that that website changed
-08:44:46 **16** something in there.

-08:44:46 **17** **Q.** Do you have an opinion as to how many times, at least
01:25:03 **18** according to this file, this computer accessed the website
01:25:07 **19** beginning 66.148?

01:25:09 **20** **A.** At least two times.

01:25:13 **21** **Q.** I'd also like to direct your attention to this part of
-08:44:46 **22** the file name here; it says Parent at 66.148.85. Then there's
-08:44:46 **23** a "2" that's in brackets there. What does that 2 in brackets
-08:44:46 **24** mean to you?

-08:44:46 **25** **A.** When a cookie is put on your computer, if one was there

-08:44:46 1 previously -- the first time it puts a bracket 1. If there is
01:25:41 2 another cookie previous to that from that same website, the
-08:44:46 3 second one has a bracket 2. So it means at some point there
-08:44:46 4 are two cookies from that website.

-08:44:46 5 Q. And this was the 2nd?

-08:44:46 6 A. Correct.

-08:44:46 7 Q. Meaning that -- well, do you have an opinion as to
01:25:59 8 whether or not this particular website, 66.148, was accessed at
-08:44:46 9 some point prior to February 28, 2005?

-08:44:46 10 A. Yes.

-08:44:46 11 Q. And was it?

-08:44:46 12 A. Yes. As the fact it's the second cookie from that
01:26:13 13 website.

01:26:14 14 Q. As long as we're talking about cookie history here, I
-08:44:46 15 just want to show you Exhibit 73. If you go to the third page
01:26:22 16 of that, are you familiar with that particular website, Mr.
-08:44:46 17 Corrigan?

-08:44:46 18 A. Yes. That was another website identified to me as being
-08:44:46 19 relevant.

-08:44:46 20 Q. Specifically with that spelling of this particular word,
01:26:43 21 E-k-h-l-a-a-s?

01:26:47 22 A. Correct.

01:26:48 23 Q. 165A1-B. And I direct your attention to page 24, and
01:27:04 24 the second item down from the top. This name here in the URL,
01:27:21 25 how does that compare to what I just showed you on Exhibit 73?

01:27:25 **1** A. It's the same address.

01:27:27 **2** MR. HARTMAN: Objection.

01:27:28 **3** THE COURT: Basis?

01:27:31 **4** MR. HARTMAN: Can we approach?

-08:44:-46 **5** THE COURT: Sure.

01:28:20 **6** (Whereupon the following discussion was had at the

-08:44:-46 **7** bench outside the hearing of the jury:)

-08:44:-46 **8** MR. HARTMAN: That clearly is not the same. There

-08:44:-46 **9** are two letters in front of the word that he's talking about.

-08:44:-46 **10** THE COURT: Why don't you ask him how he knows

-08:44:-46 **11** that.

-08:44:-46 **12** MR. HERDMAN: No problem. I can do that.

-08:44:-46 **13** (End of sidebar discussion.)

-08:44:-46 **14** BY MR. HERDMAN:

01:28:30 **15** Q. If I could direct your attention back to 73-003. 73,

01:28:40 **16** third page. This particular spelling here, what are the letters

-08:44:-46 **17** there?

-08:44:-46 **18** A. E-k-h-l-a-a-s.

01:28:50 **19** Q. Could you go back to 165A1-B, and go to page 24. Zoom

-08:44:-46 **20** in on the second there. Can you read those letters?

01:29:10 **21** A. E-k-h-l-a-a-s.

01:29:13 **22** Q. Are those the same letters that appeared on 67-003?

01:29:18 **23** MR. HARTMAN: Your Honor, I object. It's not

01:29:20 **24** complete.

01:29:21 **25** THE COURT: You testified that in your opinion

-08:44:46 1 those are the same websites, correct?

01:29:28 2 THE WITNESS: It's not the same website.

01:29:31 3 MR. HERDMAN: I didn't ask him that.

-08:44:46 4 THE COURT: I'm sorry. Why don't you ask him

-08:44:46 5 again the question that lead to the objection as to how he knows

-08:44:46 6 that answer. I think that's what the issue is, correct?

01:29:44 7 MR. HERDMAN: I'll ask a question, Your Honor.

01:29:44 8 BY MR. HERDMAN:

-08:44:46 9 Q. How do you know that those letters, E-k-h-l-a-a-s, are

-08:44:46 10 the same as appear on page 3 of Exhibit 73?

01:29:56 11 A. I know the alphabet.

01:30:06 12 MR. HERDMAN: I'm sorry, Your Honor.

01:30:13 13 THE COURT: You may continue.

01:30:16 14 BY MR. HERDMAN:

01:30:17 15 Q. Obviously this entire URL here is different than what

-08:44:46 16 was on page 3 of Exhibit 73?

-08:44:46 17 A. Correct. It's a different website.

-08:44:46 18 Q. But what does this particular item tell you with respect

-08:44:46 19 to this website called www.A-l-e-k-h-l-a-a-s.net, actually went

-08:44:46 20 to this website, www.a-l-e-k-h-l-a-a-s.net?

01:31:17 21 A. Yes, it did. At this time, and then at some time prior

01:31:23 22 to that.

-08:44:46 23 Q. At this time, you mean February 3, 2006?

-08:44:46 24 A. Correct.

-08:44:46 25 Q. As long as we're on this topic, can I direct your

-08:-44:-46 **1** attention to page 140? If you can go to the second one here.

-08:-44:-46 **2** Do you recognize that URL?

01:31:46 **3** **A.** Yes. That is what was written a couple exhibits ago.

01:31:54 **4** **Q.** Can you bring up 73-003.

01:32:13 **5** If we compare this to this, is it your opinion that

-08:-44:-46 **6** that actually is the same website?

-08:-44:-46 **7** **A.** Correct.

01:32:20 **8** **Q.** And what does this -- what does this over here tell you

-08:-44:-46 **9** about the access of this website by Exhibit 76?

01:32:30 **10** **A.** The last time that website accessed the cookie on that

01:32:36 **11** computer was 3-30 of 2005. The last time it changed it was

01:32:42 **12** 2-19 of 2005.

01:32:45 **13** **Q.** By the way, between 2-19, 2005 and 3-30, 2005, are you

-08:-44:-46 **14** able to tell whether this computer accessed this website?

-08:-44:-46 **15** **A.** Not from this. It could have been, or not.

01:33:01 **16** THE COURT: I couldn't hear you.

-08:-44:-46 **17** **A.** It could have been or could have not. I can't tell

01:33:06 **18** just from this.

01:33:08 **19** BY MR. HERDMAN:

01:33:08 **20** **Q.** What does this "2" in brackets here, this "2" in

-08:-44:-46 **21** brackets right there indicate?

-08:-44:-46 **22** **A.** It means it's the second cookie from that website.

01:33:19 **23** **Q.** So according to this right here that I've just -- on the

-08:-44:-46 **24** left there, what are the dates that you can say that Exhibit 76,

-08:-44:-46 **25** that computer, accessed this website?

01:33:32 1 A. It would be 3-30, 2005; 2-19, 2005; and sometime prior
-08:44:46 2 because it was the second cookie.

01:33:47 3 (Discussion had off the record.)

01:33:51 4 MR. HERDMAN: And then this middle one here.

01:33:59 5 BY MR. HERDMAN:

01:34:02 6 Q. Again, comparing this portion of the URL, which now
01:34:09 7 reads www.E-k-h-l-a-a-s.com, comparing that with this, do some
-08:44:46 8 of those letters appear to be the same?

-08:44:46 9 A. Yes, they are.

01:34:19 10 Q. Do you have an opinion as to whether or not the cookie
01:34:23 11 that's depicted on the left-hand side of the screen relates to
-08:44:46 12 the web page that's written on the right-hand side of the
-08:44:46 13 screen?

-08:44:46 14 A. It's the same server. It's the same IP address.

-08:44:46 15 Q. Why does the one on the left have a www in front of it?

-08:44:46 16 A. You can designate -- you can go to, like, the Yahoo.com;
-08:44:46 17 you can type in sports.Yahoo.com. It will direct you to the
-08:44:46 18 Yahoo.com sports page; or you can type mail.Yahoo.com; it will
-08:44:46 19 direct you to Yahoo.com, but it will go straight to your e-mail.
-08:44:46 20 It's just a way of segregating your site to type in something
-08:44:46 21 and then go directly to that site. www is the default. If
-08:44:46 22 you don't type anything in, it goes there automatically.

01:35:19 23 Q. This portion here on the left, what does that indicate
-08:44:46 24 with respect to Exhibit 76, the HP Vectra computer, going to
-08:44:46 25 this website, E-k-h-l-a-a-s.com?

01:35:35 **1** A. The user name of "Parent" got a cookie from that
01:35:39 **2** website. The last time that website accessed that cookie was
01:35:45 **3** 3-30, 2005. The last time it modified it was 2-17, 2005.

01:35:51 **4** Q. This bracketed "2" here?

-08:44:46 **5** A. Again, means it's the second cookie received.

01:35:57 **6** Q. Do you have an opinion as to whether or not --

01:36:02 **7** A. There was a prior access.

-08:44:46 **8** Q. -- there was prior access?

-08:44:46 **9** A. Because it is the second.

01:36:25 **10** Q. Exhibit 76-1AQ. Scroll all the way to the bottom.

01:37:00 **11** As long as this is up, I can ask you this as
-08:44:46 **12** well --

01:37:04 **13** MR. BOSS: Can we have that number again?

01:37:06 **14** MR. HERDMAN: A 76-1AQ.

01:37:14 **15** BY MR. HERDMAN:

01:37:14 **16** Q. I direct your attention to this right here. What does
01:37:18 **17** this appear to be, this exhibit?

-08:44:46 **18** A. It is the inbox for an online web page, online e-mail.

-08:44:46 **19** And in that inbox would be a message from the e-mail address of

01:37:36 **20** A-L-M-2-S-D-A at A-L-M-2-S-D-D-A.net.

-08:44:46 **21** Q. Are you familiar with the concept of encoding with
-08:44:46 **22** respect to Internet Explorer?

-08:44:46 **23** A. Yes.

-08:44:46 **24** Q. We'll get to that in a little bit. But at least the
01:37:52 **25** subject line of this e-mail, what would this subject line of the

01:37:56 1 e-mail as it appears indicate to you with respect to the
01:37:59 2 settings of Internet Explorer in terms of encoding?
-08:44:46 3 A. That the encoding is not set correctly for this web
-08:44:46 4 page.
01:38:07 5 Q. Is not set correctly?
01:38:09 6 A. Right. It should be set to something else.
01:38:15 7 Q. We'll get to this in a little bit. But I want to focus
01:38:20 8 specifically on this right here. A-L-M-2-S-D-A.net. Are you
01:38:30 9 familiar with that website?
-08:44:46 10 A. It was identified to me as being relevant.
-08:44:46 11 THE COURT: I couldn't hear you.
01:38:37 12 THE WITNESS: It was identified to me as being
-08:44:46 13 relevant.
01:38:41 14 MR. HERDMAN: If you could close that out. And go
-08:44:46 15 to page 149 of this exhibit, and the second item.
-08:44:46 16 BY MR. HERDMAN:
01:39:02 17 Q. How does this in the URL compare to that e-mail that we
01:39:09 18 just saw?
-08:44:46 19 A. It's the same domain name. It's the same server.
-08:44:46 20 Q. Do you have an opinion with respect to the dates that
-08:44:46 21 this particular website was visited by Exhibit 76?
01:39:21 22 A. The user name of "Parent" received cookie from that
-08:44:46 23 website. The last time it changed it was 2-5, 2005. The last
01:39:32 24 time it accessed it was 4-3, 2005.
01:39:35 25 Q. Meaning that Exhibit 76 went to this particular website

01:39:39 **1** on February 5, 2005?

01:39:41 **2** **A.** February 5, correct.

-08:44:46 **3** **Q.** And also on April 3, 2005?

-08:44:46 **4** **A.** Correct.

-08:44:46 **5** **Q.** And again, there's a 2 that's in brackets here?

-08:44:46 **6** **A.** Shows a prior. It was the second cookie, so there was a

-08:44:46 **7** prior cookie.

-08:44:46 **8** **Q.** Prior to February 5, 2005?

01:40:01 **9** **A.** Correct.

01:40:10 **10** MR. HERDMAN: Could we go to Exhibit 165A1.

01:40:10 **11** BY MR. HERDMAN:

-08:44:46 **12** **Q.** I just direct your attention to this third item down

-08:44:46 **13** here. What is this? Can you explain that to the jury?

-08:44:46 **14** **A.** It is the cookie for the website 66.148.85 that was

-08:44:46 **15** placed on the computer QCV-02, or Exhibit 76.

-08:44:46 **16** **Q.** What does that mean with respect to this part of your

-08:44:46 **17** report?

01:40:56 **18** **A.** That would be when the cookie was placed on the

-08:44:46 **19** computer. That would be 2-6, 2005.

01:41:03 **20** **Q.** And the modified date, what does that indicate?

-08:44:46 **21** **A.** It's the last time that that file changed in some way.

01:41:10 **22** **Q.** What about the accessed date? What would cause an

01:41:15 **23** accessed date to change?

-08:44:46 **24** **A.** Accessed dates can be changed by the user accessing it,

01:41:23 **25** as well as just the system accessing it; maybe, like, a virus

-08:-44:-46 1 scan or -- can change those dates as well. It's just the last
-08:-44:-46 2 time that file was accessed by a program or by the user.

01:41:39 3 MR. HERDMAN: If I could direct your attention

-08:-44:-46 4 now --

01:41:42 5 THE COURT: Would this be a good time for a break?

-08:-44:-46 6 MR. HERDMAN: It's fine, Your Honor.

01:41:48 7 THE COURT: We'll take our mid-morning break.

01:42:46 8 (Recess taken.)

02:14:07 9 THE COURT: You all have your notebooks, I assume.

02:14:18 10 As has happened from time to time, there's nothing

02:14:21 11 I really can do about it. I got back to my office on break,

-08:-44:-46 12 and there were a couple fairly important calls I had to tend to,

-08:-44:-46 13 and I did, and that's why we're so late getting underway. I

-08:-44:-46 14 really appreciate your patience. It comes up, and I have to

-08:-44:-46 15 deal with it. I know the one thing the jurors hate probably

-08:-44:-46 16 more than anything is sort of the hurry up and wait experience.

02:14:44 17 And I can only assure you that it's not because any of us are

02:14:53 18 lollygagging or trying to inconvenience you.

02:14:57 19 Mr. Herdman, you may continue.

-08:-44:-46 20 You remain under oath, Mr. Corrigan.

02:15:03 21 BY MR. HERDMAN:

-08:-44:-46 22 Q. Mr. Corrigan, before I get started again, I know I've

-08:-44:-46 23 been directing your attention to the monitor. When you look at

-08:-44:-46 24 the monitor, can you try to remain conscious of the fact you're

-08:-44:-46 25 looking away from the microphone, so try to coordinate it.

02:15:26 1 MR. HERDMAN: If any jurors are having any
02:15:29 2 audibility problems --
-08:44:46 3 THE COURT: If you can't hear something, let us
02:15:33 4 know, please. Okay. You may resume.
-08:44:46 5 MR. HERDMAN: Thank you, Your Honor.
02:15:37 6 BY MR. HERDMAN:
02:15:38 7 Q. Can we go back to Exhibit 165A1. This is the bookmark
-08:44:46 8 for that particular website, 66.148.
-08:44:46 9 Now, Mr. Corrigan, I asked you before whether you
02:15:57 10 were able to conduct a search for a particular URL or IP address
02:16:02 11 in all the computer evidence in this case.
02:16:04 12 A. Yes.
-08:44:46 13 Q. Did you, in fact, conduct a search for this IP address,
02:16:09 14 66.148?
-08:44:46 15 A. Yes. This bookmark shows all the accesses to that
-08:44:46 16 website across all the media that I examined.
-08:44:46 17 Q. So that includes every computer that you examined in
02:16:23 18 this case?
-08:44:46 19 A. Correct.
02:16:24 20 Q. Including Exhibit 3, a Dell laptop computer?
-08:44:46 21 A. Yes.
-08:44:46 22 Q. And the only computer that actually accessed this
-08:44:46 23 computer was Exhibit 76, an HP Vectra?
02:16:35 24 A. Correct. This specific website, yes.
02:16:39 25 Q. I direct your attention to the bottom, the file that

02:16:46 1 starts "Parent" at 66.148. There it is. Before we continue,
-08:44:46 2 I think when we left off you were talking about creation date,
-08:44:46 3 modify date, access date. Just if we could go back through
-08:44:46 4 this one more time.

-08:44:46 5 Creation date is what with respect to a cookie?

02:17:05 6 A. Creation date is when that cookie was placed on that
-08:44:46 7 computer by that website.

-08:44:46 8 Q. For instance, this one here says, with the bracketed 2
-08:44:46 9 which you testified to, the cookie that would have had a
02:17:25 10 bracketed 1, would it have had a different creation date than
-08:44:46 11 this particular cookie?

-08:44:46 12 A. It would have been prior to that.

-08:44:46 13 Q. And what about the modified date? What is that?

02:17:37 14 A. The modified date is anytime that the website or the
-08:44:46 15 user has changed the contents in that somehow.

-08:44:46 16 Q. Why would a website change the contents of a cookie?

-08:44:46 17 What does that mean exactly?

-08:44:46 18 A. To store that information that it wants to. So like I
-08:44:46 19 said before, how you went to Google.com or Yahoo.com, the sports
-08:44:46 20 page, it then creates a cookie on your computer. And then
-08:44:46 21 later on you say, I want you to remember that I like the
-08:44:46 22 Cleveland Indians. So it's going to modify that to say, next
02:18:14 23 time when you go to Yahoo Sports, show me the Cleveland Indians
-08:44:46 24 first.

02:18:19 25 Q. And the accessed date, what does that mean with respect

-08:44:46 1 to a cookie file?

-08:44:46 2 A. The file itself, since it's an actual file and it's not
-08:44:46 3 like a history entry like we were reading before, this can be
-08:44:46 4 accessed by just the regular Windows operating as well as virus
-08:44:46 5 scans. It's just any user or program accessing it. But
-08:44:46 6 inside of that history file it keeps track of when the website
02:19:01 7 accessed it.

02:19:04 8 Q. So with respect to this particular cookie again, what
-08:44:46 9 does this indicate to you with respect to the visits of this
-08:44:46 10 particular website by Exhibit 76, the HP Vectra computer?

-08:44:46 11 A. That that cookie was created or placed on the computer
-08:44:46 12 on 2-6, 2005. And the last time that that file was modified
02:19:28 13 was 2-27, 2005.

02:19:32 14 Q. And from 2-6, 2005 until 2-27, 2005, does this cookie
-08:44:46 15 provide any information as to whether that website was visited
-08:44:46 16 by Exhibit 76, the computer that's Exhibit 76?

-08:44:46 17 A. No, it does not say -- doesn't have a history of the
-08:44:46 18 times between there.

-08:44:46 19 Q. It's not like a log of times?

02:19:53 20 A. Right. It's not going to record it was modified on
-08:44:46 21 this date, this date, this date. Just the last time.

02:20:01 22 Q. So I guess just if this website had been accessed on
02:20:05 23 February 26, 2005 by this computer, when it was modified on
-08:44:46 24 February 27, 2005, the previous modification date would have
02:20:17 25 been replaced essentially?

-08:-44:-46 1 A. Correct.

-08:-44:-46 2 Q. So the modified date only indicates the last date that
02:20:23 3 this computer went to this website?

02:20:26 4 A. Not the last date it went to it. The last date
02:20:32 5 something there changed.

02:20:33 6 THE COURT: In other words, it could have been the
-08:-44:-46 7 party that applied the cookie, right?

02:20:40 8 THE WITNESS: Absolutely.

-08:-44:-46 9 THE COURT: They might have done something to
02:20:45 10 modify the cookie?

02:20:47 11 BY MR. HERDMAN:

-08:-44:-46 12 Q. Would a cookie be modified by -- I think you said before
-08:-44:-46 13 the accessed date could indicate there was some sort of system
02:20:54 14 access of a file?

-08:-44:-46 15 A. Right. It could be the system or the user accessing
-08:-44:-46 16 that file.

-08:-44:-46 17 Q. Would a modified date, would that change if there was
02:21:01 18 some sort of system access like a virus scan?

02:21:04 19 A. The only time the modified date changed is when
-08:-44:-46 20 something in that file changes. So if somebody just viewed it
-08:-44:-46 21 or accessed it for a virus scan but did not change anything
-08:-44:-46 22 there, that modified date wouldn't change.

02:21:23 23 Q. I'd like to direct your attention to Exhibit 165A-2.

02:21:36 24 Do you recognize that?

-08:-44:-46 25 A. Yes.

-08:44:46 1 Q. What is this?

02:21:40 2 A. This is the cookie from the internet history file that

-08:44:46 3 we reviewed earlier from the user name of "Parent". That is the

-08:44:46 4 second cookie that it saw that was placed.

02:21:57 5 Q. If we could try to put that on the left side of the

-08:44:46 6 screen, then on the right side bring up Exhibit 73.

02:22:13 7 Now, what does this on the left-hand side here,

-08:44:46 8 what do these creation/modification dates indicate to you?

02:22:21 9 A. That that cookie was created on 2-19, 2005. The last

-08:44:46 10 time it was modified, according to the system, is 2-19, 2005.

02:22:35 11 Q. By the way, these times that are on there, on this

-08:44:46 12 particular portion on the left-hand side, when it says 1:52

02:22:44 13 p.m., what time is that?

-08:44:46 14 A. That's Eastern Standard Time.

02:22:48 15 Q. Again, there's a 2 in brackets here on the name of the

02:22:53 16 file?

02:22:54 17 A. Yes.

02:22:55 18 Q. And this cookie relates to Exhibit 76, the HP Vectra

-08:44:46 19 computer?

-08:44:46 20 A. Correct.

-08:44:46 21 Q. Now, this is your portion of the report that discusses

-08:44:46 22 this file. But you said before that cookie file is a text

02:23:09 23 file?

-08:44:46 24 A. Correct.

-08:44:46 25 Q. So it's something you can actually open up and look at?

-08:-44:-46 **1** A. Yes, you can.

-08:-44:-46 **2** Q. I'd like to direct your attention to Exhibit 165A-2A.

-08:-44:-46 **3** Is this the actual cookie file?

02:23:30 **4** A. Correct. That is the contents of the file.

-08:-44:-46 **5** Q. And this number that's here, what is that number?

-08:-44:-46 **6** A. This website which was run by the terminology on there,

02:23:49 **7** that BB last visit. "BB last visit," which is bulletin board

02:23:59 **8** last visit. "BB last activity," which is bulletin board last

02:24:04 **9** activity. The number below that is what's called a UNIX date.

02:24:11 **10** Q. What?

02:24:12 **11** A. UNIX, U-N-I-X date.

02:24:17 **12** THE COURT: UNIX date?

02:24:19 **13** THE WITNESS: Just like the operating system.

-08:-44:-46 **14** BY MR. HERDMAN:

-08:-44:-46 **15** Q. That's a number. Is that the number that's marked with

-08:-44:-46 **16** the green dot?

-08:-44:-46 **17** A. Yes, it is.

-08:-44:-46 **18** Q. The first four digits are 1108?

-08:-44:-46 **19** A. Correct. What that is, the number of seconds since

02:24:36 **20** 1970. Now, why they picked 1970, it's probably because when

-08:-44:-46 **21** they were creating it they figured there couldn't be any files

-08:-44:-46 **22** prior to 1970 because they hadn't created that file system yet.

-08:-44:-46 **23** So they started to count at the number of seconds since January

-08:-44:-46 **24** 1 of 1970.

02:24:55 **25** Q. Do you know looking at that number what date that would

-08:44:46 1 translate into, something that we would all understand?

02:25:02 2 A. No.

-08:44:46 3 Q. How do you go about finding out what date that would

02:25:07 4 translate into?

02:25:08 5 A. There are several tools that you input the number into

-08:44:46 6 it, and it will convert that to a GMT time.

02:25:16 7 Q. Is one of them -- is there a website that will do that?

-08:44:46 8 A. Several online calculators that you might say that you

-08:44:46 9 put in the string of number; it calculates the UNIX date and --

02:25:30 10 THE COURT: You put in those numbers and they

-08:44:46 11 calculate --

02:25:33 12 THE WITNESS: What the date is in calendar format.

02:25:40 13 BY MR. HERDMAN:

02:25:41 14 Q. Did you do that in this case with respect to this

-08:44:46 15 particular -- is it a UNIX time stamp? Am I calling that

-08:44:46 16 correctly?

-08:44:46 17 A. Correct.

-08:44:46 18 Q. Did you do that in this case with respect to that UNIX

-08:44:46 19 time?

02:26:02 20 On the right put up 165A-2A-1.

-08:44:46 21 What did you do here? Can you direct the jurors to

-08:44:46 22 the two numbers that are the same here?

02:26:23 23 A. I put that number of the last visit from the bulletin

-08:44:46 24 board.

02:26:26 25 Q. Can you say what the last four digits of that number

-08:44:46 1 are?

-08:44:46 2 A. The last four digits are 3735. I put that into that
02:26:33 3 online calculator. And the date that it translated to in
02:26:39 4 calendar format would be 2-18, 2005, at 21:55 Greenwich Mean
-08:44:46 5 Time.

-08:44:46 6 Q. Do you know what the difference is between Greenwich
-08:44:46 7 Mean Time and Eastern --

-08:44:46 8 A. Five hours.

02:26:54 9 Q. So that would be -- 21:55 is what time?

02:27:05 10 A. 16 --

02:27:07 11 THE JUROR: 9:55.

02:27:09 12 BY MR. HERDMAN:

02:27:09 13 Q. 2:55 is 9:55 Greenwich Mean Time p.m. What time would
02:27:15 14 that be Eastern Standard Time?

-08:44:46 15 A. So that would be 9 --.

-08:44:46 16 Q. If Greenwich Mean Time is five hours ahead, and it's
02:27:27 17 9:55 p.m., what time would that be Eastern?

-08:44:46 18 A. Greenwich is nine? I'm sorry. I'm lost.

02:27:34 19 MR. HERDMAN: I'm not asking the question right.

02:27:37 20 Your Honor, I'll move on.

02:27:43 21 THE COURT: 21 minus five is 16. Then you convert
-08:44:46 22 that into the 12-hour clock. It would be 4:55 in the
02:27:51 23 afternoon.

-08:44:46 24 MR. HERDMAN: Thank you. Yes, Your Honor.

02:27:54 25 THE COURT: Whether I'm qualified to render that

-08:44:46 1 opinion --

02:27:58 2 MR. HERDMAN: I'll take it.

02:28:01 3 BY MR. HERDMAN:

-08:44:46 4 Q. Okay. So that's with respect to this part here, which
-08:44:46 5 is the BB last visit portion of the cookie?

-08:44:46 6 A. Correct.

-08:44:46 7 Q. Then I see the BB last activity also has a similar
-08:44:46 8 looking number there?

-08:44:46 9 A. Correct.

-08:44:46 10 Q. And is that the same UNIX time stamp?

-08:44:46 11 A. Correct. It's a different number, but yeah, it's a
02:28:23 12 UNIX time stamp.

02:28:24 13 Q. Did you run a similar calculation for that one?

-08:44:46 14 A. Yes, I did.

-08:44:46 15 Q. Could you bring up 165A-2A. 2A-2, I'm sorry.

02:28:42 16 MR. BOSS: 2A what?

-08:44:46 17 MR. HERDMAN: 2A-2.

-08:44:46 18 BY MR. HERDMAN:

02:28:51 19

02:28:51 20 Q. If you could read the last four digits from the number
-08:44:46 21 of the cookie that you ran in this calculator.

-08:44:46 22 A. The last four digits are 9332, the same number I
02:29:05 23 attributed to the calculator, and got a day of 2-19, 2005, 18:55
02:29:11 24 Greenwich Mean Time.

02:29:14 25 Q. I'm not going to get into the time calculations here.

-08:44:46 **1** A. Thank you.

-08:44:46 **2** MR. HERDMAN: Can we focus in on this part here,
-08:44:46 **3** maybe the second half of this, Kevin, below that line.

-08:44:46 **4** BY MR. HERDMAN:

02:29:31 **5** Q. What does this portion of the cookie indicate to you?

02:29:35 **6** A. Bulletin Board user ID or an ID that has been created on
-08:44:46 **7** that bulletin board of the ID of 4343 is stored on there as well
-08:44:46 **8** as the BB password, or the bulletin board password. It's that
-08:44:46 **9** encrypted hash version of the password. So this user name and
02:30:02 **10** password was stored in the cookie. So you didn't have to sign
02:30:07 **11** in for this cookie.

02:30:10 **12** Q. Again, this cookie was located on Exhibit 76, the HP
02:30:15 **13** Vectra computer?

02:30:16 **14** A. Correct.

02:30:20 **15** Q. Do all websites that ask for user ID or password
02:30:24 **16** information, do all websites that ask for such information
-08:44:46 **17** maintain a file like that in the cookie?

02:30:31 **18** A. It doesn't have to. So the answer is -- do all of
-08:44:46 **19** them? No.

02:30:37 **20** Q. So some do; some don't?

-08:44:46 **21** A. Some do. It depends on how they set up their bulletin
-08:44:46 **22** board.

02:31:19 **23** MR. HERDMAN: Your Honor, may I approach the
-08:44:46 **24** witness?

02:31:21 **25** THE COURT: Certainly.

-08:44:46 1 MR. HERDMAN: Thank you.

02:31:23 2 BY MR. HERDMAN:

-08:44:46 3 Q. Mr. Corrigan, I'm handing up a stack of compact discs.

02:31:30 4 If you'd just look through those very quickly while I make a

-08:44:46 5 record to the Court of what I've given to you.

-08:44:46 6 MR. HERDMAN: I handed up compact discs that have

02:31:43 7 been marked Government's Exhibit -- these are actually in

-08:44:46 8 evidence, Your Honor. Exhibit 14, 15, 16, 17, 18, 19, 20, 22,

02:31:56 9 23, 24, 25, 26, 29, 30, 32, 36, 38, 39, 41, 42, 46, 51, 54, 90,

02:32:19 10 101, 102, 109, 110, 111, 112, 113, 114, 115, 117, 119, as well

02:32:36 11 as two that are not yet in evidence, 57 and 58.

02:32:45 12 BY MR. HERDMAN:

02:32:45 13 Q. Mr. Corrigan, directing your attention to those items

-08:44:46 14 handed up to you, did you actually burn those CDs?

-08:44:46 15 A. Yes.

-08:44:46 16 Q. Where did you obtain the computer files you placed on

-08:44:46 17 those CDs?

-08:44:46 18 A. I wrote on the disc which evidence item I obtained that

-08:44:46 19 evidence from.

02:33:05 20 Q. What was the designation you used in terms of the

-08:44:46 21 evidence you obtained it from?

02:33:10 22 A. QCV number.

-08:44:46 23 Q. What is a QCV number?

-08:44:46 24 A. QCV numbers are the way that the FBI letters its

-08:44:46 25 evidence that it receives. Q stands for question document.

-08:44:46 1 CR is the field office, like Cleveland. And the numbers are
-08:44:46 2 just -- they append. So the first item is QCV-1, -2, and so
-08:44:46 3 forth.

02:33:43 4 Q. I want to direct your attention to some specific
02:33:46 5 evidence in this case. I'm going to ask you whether any of
-08:44:46 6 these CDs were obtained from the evidence I'm going to go
02:33:52 7 through here.

02:33:53 8 Can you bring up Exhibit 139A, please. Exhibit
02:33:59 9 139A, I see that there's a sticker on it that says QCV-140.

-08:44:46 10 Was one or more of those compact discs that I presented you
02:34:10 11 with, were files placed onto those CDs that you're holding? Are
-08:44:46 12 the QCV-140 also known as Exhibit 139A?

02:34:19 13 A. Yes.

-08:44:46 14 Q. By the way, with respect to this disc, QCV-140, Exhibit
02:34:26 15 139A, were you able to determine what date this CD was actually
-08:44:46 16 burnt?

02:34:32 17 A. Yeah. I'd have to look at my notes to refresh my
02:34:38 18 recollection.

02:34:40 19 MR. HERDMAN: Is that all right, Your Honor, if he
02:34:42 20 looks at his notes?

-08:44:46 21 THE COURT: Sure.

02:34:47 22 A. QCV-140 had a burn date of 10-19, 2005.

-08:44:46 23 BY MR. HERDMAN:

-08:44:46 24 Q. 2005?

-08:44:46 25 A. Correct.

02:35:05 1 Q. What does the actual burn date indicate?

-08:44:46 2 A. That was the day that the computer files were placed

-08:44:46 3 onto that CD.

02:35:16 4 Q. Can you explain, is it possible to burn multiple times

-08:44:46 5 onto a CD?

-08:44:46 6 A. Absolutely.

02:35:24 7 Q. How does the CD record the information?

02:35:27 8 A. If you leave the disc open, whereas you don't say this

-08:44:46 9 is all the files that are on there, you're able to create

-08:44:46 10 additional sessions on that CD. So you can add stuff to that

02:35:40 11 CD. You don't have to burn it all at once.

02:35:46 12 Q. So if I -- maybe on one day I put something on a CD and

02:35:50 13 then I say -- say it was January 1, 2005, I burnt something onto

-08:44:46 14 a CD; then on January 2 I burnt something onto the same CD;

-08:44:46 15 would that be two sessions?

02:36:01 16 A. Right. If you didn't close out the disc or say nothing

-08:44:46 17 further to be written to this disc, you are able to add stuff to

-08:44:46 18 that CD, as long as you have the space for it.

02:36:14 19 Q. Directing your attention to Exhibit 128D, that's a CD

-08:44:46 20 that's also got a sticker on it that says QCV-07?

02:36:30 21 A. Correct.

-08:44:46 22 Q. Were there -- in the stack of CDs that I handed to you,

02:36:36 23 were there one or more computer files that were burnt onto a CD

02:36:40 24 that were obtained from this Exhibit, 128D?

-08:44:46 25 A. Yes, there were.

02:36:45 1 Q. Were you able to determine what the burn date was for
02:36:49 2 this exhibit, 128D?

02:36:52 3 A. May I refer to my notes?

-08:44:46 4 MR. HERDMAN: Your Honor?

02:36:56 5 THE COURT: Yes, of course.

02:36:59 6 A. QCV-07 had the volume label of 1-11, 2005.

-08:44:46 7 BY MR. HERDMAN:

-08:44:46 8 Q. January 11, 2005?

02:37:07 9 A. Correct.

02:37:09 10 Q. Were you able to compare the files that were located on

02:37:14 11 Exhibit 128D, were you able to compare the files that were

02:37:20 12 located on that CD with other evidence that was reviewed by you

-08:44:46 13 in this case?

02:37:24 14 A. Yes.

-08:44:46 15 Q. And were you able to make any determination as to

02:37:27 16 whether or not the files on this CD were the same or similar to

-08:44:46 17 the files that were located on other CDs in the case?

02:37:36 18 A. Yes, I was. Exhibit 48 and 59 had the same times as

02:37:45 19 Exhibit 128D with the exception of one file; it was named

02:37:50 20 2usscole.zip.

02:37:54 21 Q. Can we pull up 48 and 59, and then 128D.

02:38:20 22 You said there was one file that was different.

-08:44:46 23 Where did that file reside, for lack of a better word? Is it on

02:38:29 24 128D?

-08:44:46 25 A. Yes, on 128D.

-08:44:46 1 Q. How were you able to determine that there was a
02:38:34 2 difference between one file that was on this disc as opposed to
-08:44:46 3 Exhibit 48 and 59?
02:38:41 4 A. I ran that MD hash program that generates the
02:38:45 5 fingerprint. And the fingerprint for that file was different
-08:44:46 6 between the version that's on 128D and then the 48 and 59.
-08:44:46 7 Q. So 48 and 59 were the same with regard to MD hashes?
-08:44:46 8 A. The two versions there were identical.
02:39:05 9 Q. 128D was identical with the exception of 128
02:39:10 10 usscole.zip?
02:39:12 11 A. Yes.
-08:44:46 12 Q. If you looked at all of these CDs side to side, the
02:39:16 13 actual file names, were the file names the same?
-08:44:46 14 A. Yes.
02:39:20 15 Q. In your opinion what could explain the difference in the
02:39:24 16 MD5 hash number for U.S.S. Cole on 128D?
02:39:29 17 A. There might have been a scratch on the disc or a piece
-08:44:46 18 of dust.
-08:44:46 19 THE COURT: I can't hear you.
02:39:37 20 A. A scratch on the disc, piece of dust, something that
02:39:41 21 caused that CD not to give me or to give me a different value
-08:44:46 22 for that file.
02:39:46 23 BY MR. HERDMAN:
02:39:46 24 Q. But again, all the file names for those three discs were
-08:44:46 25 the same?

-08:-44:-46 **1** A. Correct.

02:39:57 **2** Q. Pull up Exhibit 27.

02:40:09 **3** Were there files -- in the stack of CDs that are

-08:-44:-46 **4** before you, were there files burnt on the CDs by you obtained

-08:-44:-46 **5** from Exhibit 27?

02:40:36 **6** A. Yes, there was.

02:40:37 **7** Q. Were you able to determine what the burn date was for

-08:-44:-46 **8** this particular CD, Exhibit 27?

02:40:42 **9** A. 11-23, 2004.

02:40:50 **10** Q. November 23, 2004?

-08:-44:-46 **11** A. Correct.

-08:-44:-46 **12** Q. Directing your attention to 128C. There's a sticker on

-08:-44:-46 **13** there that says QCV-06. Were you able to determine --

02:41:07 **14** Actually, were there any files in that stack of CDs

-08:-44:-46 **15** before you that were obtained from Exhibit 128C?

02:41:18 **16** A. Yes, there were.

02:41:20 **17** Q. And were you able to determine what the creation date of

-08:-44:-46 **18** this particular exhibit was?

02:41:30 **19** MR. HARTMAN: Excuse me? Could we get

02:41:34 **20** clarification of what CDs we're talking about? The witness said

-08:-44:-46 **21** he burned this onto --

-08:-44:-46 **22** THE COURT: In other words, which one he created

02:41:43 **23** from this?

02:41:44 **24** MR. HARTMAN: Yes.

02:41:45 **25** THE COURT: His -- the CD which he created; can we

-08:-44:-46 **1** do that?

02:41:50 **2** MR. HERDMAN: We can do that. Can we approach
02:41:53 **3** briefly? It's not a problem.

-08:-44:-46 **4** THE COURT: Let me suggest this: Maybe we can talk
-08:-44:-46 **5** about that at lunch. It probably would be helpful to the jury
-08:-44:-46 **6** to have an equivalence list put together for everybody.

-08:-44:-46 **7** MR. HERDMAN: That's fine, Your Honor. In the
02:42:09 **8** interest of time, I'm going about this a particular way.

-08:-44:-46 **9** THE COURT: That's fine. If there's a problem, Mr.
02:42:15 **10** Hartman, we'll talk about it at lunch.

02:42:17 **11** MR. HARTMAN: That's fine.

02:42:21 **12** BY MR. HERDMAN:

02:42:22 **13** Q. We were talking about Exhibit 128C. Were you able to
-08:-44:-46 **14** determine what date this CD was burnt?

02:42:30 **15** A. It actually had five different sessions on it. The
-08:-44:-46 **16** first session --

-08:-44:-46 **17** Q. Can you remind the jury what a session is?

-08:-44:-46 **18** A. Session is you went to the disc and you added files on
-08:-44:-46 **19** to it at a later date.

02:42:45 **20** The first session was 2-6 of 2005.

02:42:51 **21** THE COURT: You may have indicated this already,
-08:-44:-46 **22** but can you determine or can you not determine what occurred on
-08:-44:-46 **23** a particular session?

02:43:02 **24** THE WITNESS: Yes, I can see what files were added.

-08:-44:-46 **25** THE COURT: What was that date again? I'm sorry; I

02:43:10 **1** interrupted.

02:43:11 **2** THE WITNESS: 2-6, 2005. The second one was 2-17,

-08:44:-46 **3** 2005. Then there was three sessions of 2-18, 2005.

02:43:21 **4** BY MR. HERDMAN:

02:43:21 **5** Q. Did you compare this particular disc, the files on this

02:43:25 **6** particular disc to any other discs or evidence that you reviewed

-08:44:-46 **7** in this case?

-08:44:-46 **8** A. Yes.

-08:44:-46 **9** Q. And did there appear to be similarities between the

-08:44:-46 **10** files contained on this disc and another piece of evidence that

-08:44:-46 **11** you reviewed in this case?

-08:44:-46 **12** A. Exhibit Number 60 contained the first session of Exhibit

02:43:49 **13** 128C, QCV-06.

-08:44:-46 **14** Q. That was the session created on February 6, 2005?

02:43:57 **15** A. Correct.

02:43:59 **16** Q. I'd like to direct your attention now to Exhibit 120.

02:44:14 **17** MR. HARTMAN: The identifying number?

-08:44:-46 **18** BY MR. HERDMAN:

-08:44:-46 **19** Q. There's testimony to this, too. Looking at Exhibit 120,

02:44:32 **20** it's not a CD obviously. What is that thing?

-08:44:-46 **21** A. That's called a USB drive.

-08:44:-46 **22** Q. Can you explain to the jury what this is as opposed to a

02:44:43 **23** CD?

-08:44:-46 **24** A. USB drive is kind of like the grown-up version of

02:44:47 **25** floppies. Instead of having just one megabyte, this USB drive,

02:44:53 **1** which you plug into the USB port on the computer, it's kind of
-08:-44:-46 **2** like a mini hard drive. It has a larger capacity to store
-08:-44:-46 **3** things onto. This one is 512 megabyte. It would hold
02:45:07 **4** approximately 500 floppies worth of information.

02:45:11 **5** **Q.** Did you obtain any of the disks in the stack of CDs
-08:-44:-46 **6** before you -- were any of those obtained from --

02:45:18 **7** MR. HARTMAN: Your Honor, may we approach?
-08:-44:-46 **8** THE COURT: Sure.

02:45:20 **9** (Whereupon the following discussion was had at the
02:47:09 **10** bench outside the hearing of the jury:)

02:47:09 **11** MR. HARTMAN: I think Agent Gubanich testified
-08:-44:-46 **12** yesterday that he didn't remember where he got this. So I
-08:-44:-46 **13** don't think there's any foundation for testimony about what's on
-08:-44:-46 **14** it.

-08:-44:-46 **15** MR. HERDMAN: There's plenty of foundation. Agent
-08:-44:-46 **16** Gubanich isn't the only person who can lay a foundation for this
-08:-44:-46 **17** particular exhibit. It's in evidence.

-08:-44:-46 **18** THE COURT: I believe the foundation has been laid,
-08:-44:-46 **19** where it came from.

-08:-44:-46 **20** MR. HERDMAN: It's been admitted into evidence.
-08:-44:-46 **21** And there's testimony from -- I can think of at least two
-08:-44:-46 **22** witnesses that have testified with respect to this exhibit.

-08:-44:-46 **23** THE COURT: Yeah.

-08:-44:-46 **24** MR. BOSS: Who was that?

-08:-44:-46 **25** THE COURT: Let me say this: If you want to go

-08:44:46 1 back to the record and determine whether or not that is so, then
-08:44:46 2 you can renew your objection. It's my recollection it's in
-08:44:46 3 evidence; and therefore, whether there's a foundation or not, I
-08:44:46 4 don't think that really matters because it's in evidence. Even
-08:44:46 5 so, it's my recollection as to all of these things there was an
-08:44:46 6 adequate foundation.

-08:44:46 7 (End of side-bar discussion.)

02:47:20 8 THE COURT: Once again, ladies and gentlemen, if
-08:44:46 9 you can't hear something, feel as free as I do to interrupt and
-08:44:46 10 say speak up.

02:47:30 11 Go ahead, Mr. Herdman.

02:47:35 12 BY MR. HERDMAN:

02:47:36 13 Q. You explained what a thumb drive is. When a file is
-08:44:46 14 placed onto a thumb drive generally, how does the thumb drive
-08:44:46 15 deal with data creation that's placed -- a file that's placed
02:47:49 16 onto that thumb drive?

-08:44:46 17 A. The data creation is just when that specific file was
-08:44:46 18 placed on it. So it creates a new copy of the file. It's going
-08:44:46 19 to update creation date at that time.

-08:44:46 20 Q. So if the creation date on a computer, like a hard drive
-08:44:46 21 of a computer, was January 1, 2005, and then I took that file
02:48:13 22 and put it onto a thumb drive on June 1, 2005, what would be the
-08:44:46 23 creation date with respect to the file as it existed on the
-08:44:46 24 thumb drive?

-08:44:46 25 A. It would be the day you placed it on there.

-08:44:46 **1** Q. June 1, 2005?

-08:44:46 **2** A. Right.

02:48:31 **3** Q. Were there files that you obtained off of Exhibit 120

-08:44:46 **4** that were then burnt onto a CD in this stack that's before you

-08:44:46 **5** there?

02:48:41 **6** A. Yes, there is.

02:48:44 **7** Q. Were some of the files on the CDs before you, were some

-08:44:46 **8** of those files recovered from Exhibit 124? It's a Sony Vaio

02:48:54 **9** laptop. It's also marked with a sticker that says QCV-14.

-08:44:46 **10** A. Yes.

-08:44:46 **11** Q. Were some of the files in those CD exhibits recovered

-08:44:46 **12** from Exhibit 136?

02:49:09 **13** A. Yes, there were.

-08:44:46 **14** Q. That's a computer tower that has the letters ECS on

02:49:18 **15** there.

02:49:20 **16** Was it your opinion -- I'm talking about the CDs in

02:49:23 **17** front of you. With respect to the location of files that you

-08:44:46 **18** burnt onto those CDs, did you have an opinion as to whether or

02:49:29 **19** not those files existed in multiple locations in the computer

02:49:33 **20** evidence?

-08:44:46 **21** A. Yes. I documented where the duplications are in my

-08:44:46 **22** report.

02:49:38 **23** Q. And were some of those files on several different CDs?

02:49:43 **24** A. Absolutely.

-08:44:46 **25** Q. Did some of those files exist on CDs and hard drives?

-08:44:46 **1** **A.** Correct.

-08:44:46 **2** **Q.** I have one last disc to ask you about. This is Exhibit
02:49:55 **3** 139B. It's marked with a sticker that says QCV-167. Were you
-08:44:46 **4** able to determine the creation date or the burn date of that
-08:44:46 **5** particular disc?

-08:44:46 **6** **A.** This has two sessions again. So additional data was
02:50:15 **7** added to it on -- both on the same date, and that was 5-13,
02:50:21 **8** 2004.

-08:44:46 **9** **Q.** May 13, 2004?

-08:44:46 **10** **A.** Correct.

02:50:27 **11** MR. HERDMAN: And I have one hard drive or one
02:50:29 **12** computer to ask you about. It's Exhibit 127. And that -- if
-08:44:46 **13** you could zoom in on the top. Is there a particular designation
-08:44:46 **14** on the top of that computer?

02:50:44 **15** MR. WITMER-RICH: Mr. Herdman, can you briefly show
02:50:48 **16** 139B again?

02:50:53 **17** MR. HERDMAN: Sure.

02:51:01 **18** (Exhibit shown.)

02:51:06 **19** MR. WITMER-RICH: Thank you.

02:51:06 **20** BY MR. HERDMAN:

02:51:18 **21** **Q.** 127. What are the letters on this; there, on this
02:51:23 **22** computer?

-08:44:46 **23** **A.** TDK.

02:51:24 **24** **Q.** On this TDK computer tower, did you take any files off
-08:44:46 **25** this particular Exhibit 127 and burn them onto one of the CDs

-08:44:46 **1** that you created for this case?

-08:44:46 **2** **A.** Yes.

-08:44:46 **3** **Q.** Did you review the hard drive of this computer, Mr.

-08:44:46 **4** Corrigan?

02:51:52 **5** **A.** Yes, I did.

02:51:53 **6** **Q.** What were you able to determine with respect to this

02:51:55 **7** particular hard drive?

-08:44:46 **8** **A.** The hard drive was reformatted on 1-30, 2006, and had a

-08:44:46 **9** partial installation of Windows.

02:52:09 **10** **Q.** What does that mean?

02:52:11 **11** **A.** It means the hard drive was reformatted, and a new

-08:44:46 **12** version of Windows was placed on it on 1-30, 2006.

-08:44:46 **13** **Q.** What effect did that have on the actual hard drive

-08:44:46 **14** itself?

02:52:31 **15** **A.** All the files that were previously on it, in that

02:52:35 **16** volume, were then erased. And then new -- a new version of

02:52:41 **17** Windows and its new files were placed on it.

02:52:50 **18** **Q.** Regarding all the exhibits we've just discussed, both

-08:44:46 **19** the CDs and the computer towers and the CDs that are in front of

-08:44:46 **20** you, did you record the locations of the files that were burnt

-08:44:46 **21** onto those particular CDs?

-08:44:46 **22** **A.** Yes, I did.

-08:44:46 **23** **Q.** And did you place -- how did you record the locations of

-08:44:46 **24** those files?

-08:44:46 **25** **A.** I created a CD that has the information from the file,

-08:44:46 1 which was Exhibit 165E, as well as I wrote on the disc where it
02:53:25 2 came from, the file that I got, and then a description of the
-08:44:46 3 file.

02:53:31 4 Q. So 165E contains essentially the locations of all of the
02:53:37 5 RD-exhibits that are before you that I made a record of earlier?

-08:44:46 6 A. Correct.

-08:44:46 7 Q. They exist in what format?

02:53:44 8 A. As a text file.

-08:44:46 9 MR. HERDMAN: Your Honor, I've already offered --

02:53:48 10 THE COURT: I did not hear the answer.

02:53:50 11 THE WITNESS: A text file.

02:53:52 12 MR. HERDMAN: I've already offered that exhibit
-08:44:46 13 into evidence, Your Honor. I think it's been admitted. I can
02:54:09 14 take away the stack of CDs.

02:54:11 15 Can I approach the witness, Your Honor?

02:54:13 16 THE COURT: Sure.

-08:44:46 17 MR. HERDMAN: I want to pinpoint a couple specific
-08:44:46 18 files in this case. Can you bring up Exhibit 165A-3. Zoom in
02:54:48 19 on the top there. Zoom in on both.

02:54:59 20 BY MR. HERDMAN:

-08:44:46 21 Q. This particular exhibit, do you recognize this?

-08:44:46 22 A. Yes, it's a portion of my report.

02:55:04 23 Q. And what does this -- what specific file does this deal
-08:44:46 24 with?

02:55:12 25 A. The file name is baroodaswad, then some characters that

02:55:26 **1** would indicate Arabic or some other language encoding, WMV.

02:55:34 **2** Q. These characters here?

-08:44:46 **3** A. Correct.

-08:44:46 **4** Q. If you wanted to locate the original Arabic text of this

-08:44:46 **5** file, how would you go about doing this?

-08:44:46 **6** A. I would go to the spreadsheet I created that had what

02:55:47 **7** FTK called that item and what it would have appeared on the

-08:44:46 **8** computer as.

-08:44:46 **9** Q. So would you do that based on this number here?

-08:44:46 **10** A. Absolutely.

02:55:56 **11** Q. Can you go to Exhibit 165D-1. Go to page 46. Do you

-08:44:46 **12** see that file on this page, Mr. Corrigan?

-08:44:46 **13** A. Yes, I do.

-08:44:46 **14** Q. Can you just hit it on the screen there so everyone can

-08:44:46 **15** see it?

02:56:32 **16** How would you retrieve the original Arabic file

02:56:36 **17** name of that particular file?

02:56:38 **18** MR. BOSS: Was a particular file identified?

02:56:47 **19** MR. HERDMAN: Can you do it bigger?

-08:44:46 **20** THE COURT: The upper left, 102.

02:56:53 **21** BY MR. HERDMAN:

02:56:53 **22** Q. No, there's a number there, 1024804. That number is

02:57:02 **23** what?

-08:44:46 **24** A. The FTK item number.

-08:44:46 **25** Q. You see the number Baroodaswad.wmv that's been

-08:-44:-46 1 underlined?

02:57:15 2 A. Correct.

02:57:27 3 Q. Going to that third column there, can you explain for

-08:-44:-46 4 the jurors what a file path is and how your software preserves a

-08:-44:-46 5 file path?

02:57:38 6 THE COURT: File --

02:57:39 7 MR. HERDMAN: -- path, Your Honor.

02:57:40 8 A. A file path is the exact location where that file is.

-08:-44:-46 9 And if you're familiar with your computer, you go to My

02:57:50 10 Computer, hit C:, which is your hard drive. You have a

02:57:58 11 documents, settings folder, your user name, then the Desktop.

02:58:02 12 Full path is just all of those directories in front of that

02:58:06 13 showing exactly where on the hard drive, where in the file

-08:-44:-46 14 system that file is located.

02:58:14 15 BY MR. HERDMAN:

02:58:14 16 Q. Using the example of what's in the third column here,

-08:-44:-46 17 can you walk through with the jurors what this file path would

-08:-44:-46 18 be?

02:58:22 19 A. Right. So --

02:58:24 20 Q. Let me stop you just a second. I'm just going to zoom

02:58:30 21 in on that portion of it.

02:58:33 22 A. This first bit of information using this program is just

-08:-44:-46 23 what I'd call the case. CV69185 and CV69440.

02:58:48 24 THE COURT: When you rattle those off, if you could

-08:-44:-46 25 do so a little more slowly. CV69185_CV69440.

02:58:59 **1** THE COURT: That is what?

02:59:01 **2** THE WITNESS: That's what I call the case that I

-08:44:46 **3** made of this product. The next item, 69185_C14 is the

02:59:15 **4** designation of the evidence item or the hard drive that it came

-08:44:46 **5** from, which I believe is the Sony Vaio, which is an Exhibit 124.

02:59:31 **6** F is just -- it would have been the fourth partition that this

02:59:39 **7** software saw. So everything after that would be the actual

-08:44:46 **8** directories on the computer. So on the computer, it would have

-08:44:46 **9** been this Arabic text/new folder 2/new folder 3/Arabic text/,

03:00:01 **10** then the baroodaswad.wmv. Then Arabic text.wmv.

03:00:10 **11** Q. This is the text baroodaswad.wmv?

03:00:16 **12** A. Correct.

-08:44:46 **13** Q. It consisted inside a directory or folder with an Arabic

03:00:21 **14** name?

-08:44:46 **15** A. Correct.

-08:44:46 **16** Q. Then that directory with an Arabic name rested inside

-08:44:46 **17** this directory called New Folder 3?

-08:44:46 **18** A. Correct.

-08:44:46 **19** Q. Then that directory called New Folder 3 rested inside a

03:00:32 **20** directory called New Folder 2?

-08:44:46 **21** A. Correct.

-08:44:46 **22** Q. Which rested inside a directory with another Arabic

-08:44:46 **23** name?

-08:44:46 **24** A. Right, on the fourth partition.

-08:44:46 **25** Q. When you say "fourth partition", you're talking about

03:00:45 **1** this letter F here?

-08:-44:-46 **2** A. Yeah. Partition is if you have a hard drive, you can
-08:-44:-46 **3** segregate the hard drive so you can put, like, a C: and a D: is
03:00:58 **4** all on your hard drive. A lot of times people use it to
03:01:02 **5** segregate stuff that they want to keep separate. So businesses
03:01:05 **6** use it because they can keep all their applications on C: and
-08:-44:-46 **7** keep all their Word documents on D:. It's just a way to further
-08:-44:-46 **8** segregate a computer hard drive into smaller more easily
03:01:22 **9** understandable chunks.

03:01:26 **10** Q. If you can go back out to Exhibit 165A-3, can you see a
-08:-44:-46 **11** portion of what you just went through, the file path? Can you
03:01:47 **12** actually see a portion of that in your report here that was
03:01:50 **13** preserved by Forensic Toolkit?

-08:-44:-46 **14** A. Yes.

03:01:54 **15** Q. It's the Arabic text that you have to go through that
03:01:57 **16** spreadsheet for?

-08:-44:-46 **17** A. Correct.

03:02:00 **18** Q. Now, with respect to this first instance here in your
-08:-44:-46 **19** report of this file, do you notice -- I notice there's a
-08:-44:-46 **20** creation date; it says February 5, 2005.

03:02:19 **21** A. Yes.

03:02:22 **22** Q. And you said that this related to Exhibit No. 124, which
-08:-44:-46 **23** is the Sony Vaio laptop?

-08:-44:-46 **24** A. That's correct.

-08:-44:-46 **25** Q. During the course of your examination and your analysis

-08:44:46 1 in this case, were you able to determine anything with respect
-08:44:46 2 to the clock on that Exhibit 124, the Sony Vaio?

-08:44:46 3 A. Yes. When I examined the computer, I discovered that
03:02:46 4 on 1-30 of 2006 the clock had been changed to a previous date at
-08:44:46 5 that time.

03:02:58 6 Q. Let me draw your attention to Exhibit 165A-4. Is this
03:03:09 7 a bookmark from your report?

-08:44:46 8 A. Yes, it is.

-08:44:46 9 Q. It says: C14, clock discrepancy?

-08:44:46 10 A. Correct.

-08:44:46 11 Q. C14, I think you just testified, is Exhibit 124?

-08:44:46 12 A. Yes.

-08:44:46 13 Q. Which is the Sony Vaio laptop. What is this on the
03:03:25 14 screen here? Can you explain that for us?

-08:44:46 15 A. All right. So Windows, when you're using it, it will
03:03:31 16 periodically go out and check for updates. If you've used a
03:03:40 17 computer, and using it, it will say there are three updates for
-08:44:46 18 your download so that you can update the latest security
03:03:47 19 settings and so on. What this program is called, Windows
-08:44:46 20 Update, this keeps a log on your computer of every time that it
-08:44:46 21 checks for updates. So when the first time it checks for
-08:44:46 22 updates, it's going to record the time and the date of when it
03:04:06 23 checked for an update. And it always will be sequential; that
03:04:13 24 is, you'll never have, in a normal operating clock, a date
03:04:23 25 say -- say you checked it, say it says January 1st I checked for

-08:44:46 **1** updates, January 2nd I checked for updates. It should not say
03:04:34 **2** January 1st I checked for updates again, because it's
03:04:38 **3** sequential. So if you see that, that's an indication that the
-08:44:46 **4** clock had been altered on the computer. And in this case it
-08:44:46 **5** had. And it was --

03:04:53 **6** **Q.** I'm going to draw your attention to Exhibit 165A-4A.

-08:44:46 **7** If you go to page 318. Can you, taking a look at that, Mr.
-08:44:46 **8** Corrigan, do you see anything unusual about that -- before I ask
-08:44:46 **9** that question, what is this thing that we're actually looking at
-08:44:46 **10** here?

03:05:41 **11** **A.** That is the contents of that Windows Update log.

-08:44:46 **12** **Q.** So this is the actual log as it would be printed out?

-08:44:46 **13** **A.** Correct.

-08:44:46 **14** **Q.** Now, looking at this log, do you see anything unusual
03:05:51 **15** about the way that the log progresses down the page?

-08:44:46 **16** **A.** Right. So if you see the top, it says the computer --
-08:44:46 **17** the computer clock was set at 2006, 01 -- January 30, and
03:06:07 **18** checked for updates. Then about three-quarters down the page
03:06:16 **19** you'll see again that same date.

-08:44:46 **20** THE JUROR: Can you make that a little bigger?

03:06:32 **21** MR. HERDMAN: I'm going to zoom in on the bottom
-08:44:46 **22** half.

03:06:45 **23** BY MR. HERDMAN:

03:06:46 **24** **Q.** You were explaining the progression.

03:06:50 **25** **A.** Right. You see a checking for update on 2006, January

-08:-44:-46 **1** 30, 19:32:34.

03:07:06 **2** Q. Feel free to mark the screen so everyone can follow
03:07:10 **3** along here.

03:07:11 **4** A. Right there.

-08:-44:-46 **5** The next time it checked for updates the computer
-08:-44:-46 **6** thought it was 2005. 01-30, which is a year previous to that.

03:07:25 **7** Q. In your review of the evidence in this case, was there
03:07:29 **8** anything else that occurred on January 30, 2006, with respect to
03:07:34 **9** one of the computers?

-08:-44:-46 **10** A. The same day that the TDK, which is Exhibit 127, was
03:07:44 **11** reformatted.

-08:-44:-46 **12** Q. Do you have any opinion as to what would cause this date
03:07:49 **13** discrepancy here from 2006 to 2005?

-08:-44:-46 **14** A. There really is no way to say; the possible -- for sure
-08:-44:-46 **15** how that got changed unless you were there. Possible scenarios
03:08:05 **16** of how the change could have been --

03:08:07 **17** MR. HARTMAN: Objection.

03:08:08 **18** THE COURT: Well, are you about to testify to the
03:08:15 **19** different ways in which that could have occurred?

03:08:18 **20** THE WITNESS: Yes.

03:08:19 **21** THE COURT: And is that based upon your background
-08:-44:-46 **22** and experience?

03:08:26 **23** THE WITNESS: Absolutely.

-08:-44:-46 **24** THE COURT: And will you be testifying as to all
-08:-44:-46 **25** the ways in which that could have occurred?

-08:-44:-46 **1** THE WITNESS: Yes.

03:08:32 **2** THE COURT: So you're not speculating?

-08:-44:-46 **3** THE WITNESS: Right.

-08:-44:-46 **4** THE COURT: You're simply stating --

-08:-44:-46 **5** MR. HARTMAN: Withdraw the objection.

-08:-44:-46 **6** THE COURT: That's fine. No problem.

03:08:39 **7** THE WITNESS: The first way, possible way it could

-08:-44:-46 **8** have been would have been the computer clock was changed by the

03:08:51 **9** user.

-08:-44:-46 **10** The second way a program can change, a sufficient

03:08:58 **11** level program can change the clock. As well as just a hardware

03:09:04 **12** failure could possibly change the clock on the computer.

03:09:09 **13** The reason I wouldn't say hardware failure so

-08:-44:-46 **14** much --

03:09:16 **15** MR. WITMER-RICH: Objection, Your Honor.

03:09:18 **16** THE COURT: I could not hear the answer. Then

-08:-44:-46 **17** I'll hear the objection. What did you just say?

03:09:25 **18** THE WITNESS: The reason why I would discount

03:09:28 **19** hardware failure.

-08:-44:-46 **20** MR. WITMER-RICH: Objection.

-08:-44:-46 **21** THE COURT: Okay. Do you want to approach for a

03:09:33 **22** moment?

03:09:33 **23** (The following discussion was had at the bench

03:10:57 **24** outside the hearing of the jury:)

03:10:57 **25** THE COURT: Do you know what he's going to say?

-08:44:46 1 MR. HERDMAN: I have no idea what he's going to
-08:44:46 2 say. That's not --
-08:44:46 3 MR. WITMER-RICH: That makes two of us.
-08:44:46 4 MR. HERDMAN: Only because I've prepped him for
-08:44:46 5 this, we've talked about it. But I don't really remember what
-08:44:46 6 it was specifically.

-08:44:46 7 THE COURT: Can he testify to this to a reasonable
-08:44:46 8 degree of forensic computer certainty as to why he would
-08:44:46 9 discount that or explain that?

-08:44:46 10 MR. HERDMAN: Absolutely.

-08:44:46 11 THE COURT: Okay.

-08:44:46 12 MR. HERDMAN: My guess is, I think it's going to be
-08:44:46 13 something relatively benign that he's going to explain. If
-08:44:46 14 not, I can come back up.

-08:44:46 15 THE COURT: If not, not. I'll instruct the jury
-08:44:46 16 to forget about it.

-08:44:46 17 (End of side-bar discussion.)

03:11:02 18 THE COURT: The witness can answer.

03:11:07 19 THE WITNESS: The reason I would discount hardware
03:11:10 20 failure would be typically when a hardware failure occurs, the
03:11:14 21 clock is reset to January 1 of 1900, or whenever the BIOS --
03:11:30 22 B-I-O-S, BIOS, is the way the operating system like Microsoft
03:11:33 23 Window communicates. It allows the communication between the
03:11:37 24 hardware and your operating system. So that's responsible for
-08:44:46 25 keeping the system clock. Typically when that's set, it will

03:11:48 **1** default to January 1 at midnight, zero, zero, zero, zero. And
-08:-44:-46 **2** in this case it was changed to a specific day in 2005.

03:12:03 **3** BY MR. HERDMAN:

03:12:03 **4** **Q.** So with respect to files that were created or modified
-08:-44:-46 **5** on Exhibit 124, the Sony Vaio laptop, if they occurred after
-08:-44:-46 **6** January 30 of 2006 in real time as opposed to the computer's
03:12:21 **7** time, how would the computer designate their creation date or
-08:-44:-46 **8** their modification date?

-08:-44:-46 **9** **A.** I wouldn't have any confidence in those dates because
03:12:31 **10** while the date was set a year exactly, say it was set a year
-08:-44:-46 **11** back, but there's nowhere there on that that says it was set --
-08:-44:-46 **12** this is what the real actual time is, and then this is what I am
-08:-44:-46 **13** set to. So you can't really say that that file has or that
03:12:52 **14** date it was sent to is exactly a year off or any amount of a
-08:-44:-46 **15** year off. It's just off.

03:12:59 **16** **Q.** Were you able to examine this Exhibit 124, the laptop,
-08:-44:-46 **17** with respect to activity occurring early in 2005?

03:13:12 **18** **A.** Yes, I was.

03:13:14 **19** **Q.** Do you have any opinion to the relative degree of use of
-08:-44:-46 **20** this computer as of, say, February or March of 2005?

03:13:25 **21** MR. WITMER-RICH: Objection, Your Honor.

03:13:29 **22** THE COURT: Foundation?

-08:-44:-46 **23** MR. WITMER-RICH: Relative degree of use.

03:13:33 **24** THE COURT: Why don't you rephrase.

03:13:35 **25** MR. HERDMAN: I can rephrase it, Your Honor.

-08:-44:-46 **1** BY MR. HERDMAN:

-08:-44:-46 **2** Q. What was one of the things that you analyzed with
03:13:39 **3** respect to Exhibit 124 in terms of the use, the use of the
03:13:43 **4** computer?

03:13:45 **5** A. I examined the internet history of the computer. I
03:13:50 **6** examined when it was -- when the operating system says it was
03:13:58 **7** installed, and other things.

-08:-44:-46 **8** Q. And were you able to locate a general timeframe in which
03:14:06 **9** this computer was being used more often?

03:14:10 **10** A. Around September of 2005.

03:14:13 **11** Q. And then continuing forward?

03:14:15 **12** A. Correct.

03:14:20 **13** MR. HERDMAN: Can we go back to Exhibit 165A-3.

03:14:35 **14** BY MR. HERDMAN:

03:14:36 **15** Q. So directing your attention --

-08:-44:-46 **16** THE COURT: Would this be a good point to break, if
03:14:42 **17** you're winding something up?

-08:-44:-46 **18** MR. HERDMAN: I am, Your Honor. Just two more
-08:-44:-46 **19** minutes, then I'll be done with this part of it at least.

03:14:49 **20** BY MR. HERDMAN:

-08:-44:-46 **21** Q. With respect to these two parts of your report here
-08:-44:-46 **22** relating to the file barood aswad, you said these were both
-08:-44:-46 **23** located on Exhibit 24?

-08:-44:-46 **24** A. Correct.

03:15:01 **25** Q. And I notice that there is -- the second one here has a

-08:44:46 1 creation date of 11-10, 2005?

-08:44:46 2 A. Correct.

-08:44:46 3 Q. And then the first one here has a creation date of

-08:44:46 4 February 5, 2005?

03:15:15 5 A. Correct.

03:15:18 6 Q. Based on your evaluation of the clock on the Sony Vaio

03:15:23 7 laptop, do you have any opinion as to whether that file, the

-08:44:46 8 baroodaswad.wmv, could have been created after January 30, 2006?

03:15:34 9 A. Right. I don't know what date that was in actuality,

03:15:38 10 but I know during this time period the clock was inaccurate.

03:15:42 11 Q. It was inaccurate in a way that it was recording the

-08:44:46 12 dates as if they occurred a year prior or thereabouts?

-08:44:46 13 A. Right.

03:15:52 14 MR. WITMER-RICH: Objection.

03:15:53 15 THE COURT: Sustained. I think he testified he

03:15:55 16 couldn't be that sure. Or if he can be -- if he can answer

03:16:02 17 that, then let's find out why again.

03:16:06 18 MR. HERDMAN: If I can just take a minute, Your

03:16:08 19 Honor.

03:16:09 20 BY MR. HERDMAN:

03:16:10 21 Q. This file here that's -- the second one,

-08:44:46 22 baroodaswad.wmv, what's the creation date on that file?

03:16:18 23 A. 11-10 of 2005.

03:16:21 24 Q. What's the modified date of this file?

03:16:23 25 A. 11-6, 2005.

-08:-44:-46 1 Q. And what does it indicate is the accessed date of that
-08:-44:-46 2 file?

03:16:29 3 A. 12-5, 2005.

03:16:33 4 Q. And is it possible that a file could have an access date
03:16:37 5 prior to the creation date on a hard drive?

03:16:43 6 A. An access date prior to a creation date, very unlikely.

03:16:49 7 MR. BOSS: Pardon me?

-08:-44:-46 8 THE COURT: Very unlikely, he said.

03:16:54 9 MR. HERDMAN: I can stop there.

03:17:03 10 THE COURT: Let's take our noon hour recess and try
-08:-44:-46 11 to resume at 1:00.

12 (Lunch recess taken.)

13 - - -

14

15

16 C E R T I F I C A T E

17

18 I certify that the foregoing is a correct transcript from the
19 record of proceedings in the above-entitled matter.

20

21 /s Tracy L. Spore

22 Tracy L. Spore, RMR, CRR

Date

23

24

25